

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Hideo SATO

GAU:

SERIAL NO: New Application

EXAMINER:

FILED: Herewith

FOR: ENCRYPTION APPARATUS

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS  
ALEXANDRIA, VIRGINIA 22313

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number \_\_\_\_\_, filed \_\_\_\_\_, is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e):  
Application No. \_\_\_\_\_ Date Filed \_\_\_\_\_
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY

APPLICATION NUMBER

MONTH/DAY/YEAR

Japan

2002-214281

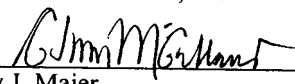
July 23, 2002

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. \_\_\_\_\_ filed \_\_\_\_\_
- ☐ were submitted to the International Bureau in PCT Application Number \_\_\_\_\_  
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. \_\_\_\_\_ filed \_\_\_\_\_; and
- ☐ (B) Application Serial No.(s) \_\_\_\_\_  
☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.

  
\_\_\_\_\_  
Gregory J. Maier

Registration No. 25,599



22850

Tel. (703) 413-3000  
Fax. (703) 413-2220  
(OSMMN 05/03)

C. Irvin McClelland  
Registration Number 21,124

日本国特許庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application:

2002年 7月23日

出願番号

Application Number:

特願2002-214281

[ ST.10/C ]:

[ JP 2002-214281 ]

出願人

Applicant(s):

ソニー株式会社

2003年 6月 2日

特許庁長官  
Commissioner,  
Japan Patent Office

太田信一郎

出証番号 出証特2003-3042461

【書類名】 特許願

【整理番号】 0290074101

【提出日】 平成14年 7月23日

【あて先】 特許庁長官 殿

【国際特許分類】 G09C 1/00  
H04L 9/30  
H04L 9/06  
H04B 1/38

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
内

【氏名】 佐藤 英雄

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100110434

【弁理士】

【氏名又は名称】 佐藤 勝

【手数料の表示】

【予納台帳番号】 076186

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0011610

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号化装置

【特許請求の範囲】

【請求項 1】 公開鍵暗号化方式による暗号化処理を行う暗号化装置であって、

演算用の値を保持するためのレジスタ及び結果を取り込むためのレジスタからなるレジスタ群を有し、公開鍵暗号化方式による暗号化処理を行う公開鍵暗号化処理手段と、

上記公開鍵暗号化処理手段によって用いるハッシュ値を生成するハッシュ値生成手段とを備え、

少なくとも、上記ハッシュ値生成手段における演算用の値を保持するためのレジスタ及び結果としてのハッシュ値を取り込むためのレジスタからなるレジスタ群を、上記公開鍵暗号化処理手段における上記レジスタ群と共用し、処理モードに応じて、動作させるハードウェアを時分割に切り替えること

を特徴とする暗号化装置。

【請求項 2】 上記公開鍵暗号化処理手段によって暗号化処理を行う際に必要となる乱数を生成するために、共通鍵暗号化方式による暗号化処理を行う共通鍵暗号化処理手段を備え、

上記共通鍵暗号化処理手段におけるデータを保持するレジスタ及び鍵データを保持するレジスタからなるレジスタ群を、上記公開鍵暗号化処理手段における上記レジスタ群と共用すること

を特徴とする請求項 1 記載の暗号化装置。

【請求項 3】 上記共通鍵暗号化処理手段は、DES暗号化処理を行うことを特徴とする請求項 2 記載の暗号化装置。

【請求項 4】 上記公開鍵暗号化処理手段は、公開鍵暗号化方式による暗号化処理に際する各種演算処理を行う公開鍵暗号化演算処理コア手段を有し、

上記ハッシュ値生成手段は、上記ハッシュ値の生成処理に際する各種演算処理を行うハッシュ値演算処理コア手段を有し、

上記公開鍵暗号化演算処理コア手段と、上記ハッシュ値演算処理コア手段とを

共用すること

を特徴とする請求項 1 記載の暗号化装置。

【請求項 5】 上記公開鍵暗号化演算処理コア手段における加算手段と、上記ハッシュ値演算処理コア手段における加算手段とを共用すること

を特徴とする請求項 4 記載の暗号化装置。

【請求項 6】 上記公開鍵暗号化処理手段は、ビット幅を可変とするためのバス切り替えスイッチを有し、

上記ハッシュ値生成手段におけるバス切り替えスイッチを、上記公開鍵暗号化処理手段における上記バス切り替えスイッチと共用すること

を特徴とする請求項 1 記載の暗号化装置。

【請求項 7】 上記公開鍵暗号化処理手段によって暗号化処理を行う際に必要となる乱数を生成するために、共通鍵暗号化方式による暗号化処理を行う共通鍵暗号化処理手段を備え、

上記共通鍵暗号化処理手段におけるバス切り替えスイッチを、上記公開鍵暗号化処理手段における上記バス切り替えスイッチと共用すること

を特徴とする請求項 6 記載の暗号化装置。

【請求項 8】 上記ハッシュ値生成手段によって生成されたハッシュ値を格納する記憶手段を備え、

上記ハッシュ値生成手段は、生成したハッシュ値を上記記憶手段に格納する際に、上記公開鍵暗号化処理手段によって用いられるアドレスに当該ハッシュ値を格納し、

上記公開鍵暗号化処理手段は、上記記憶手段に格納されたハッシュ値を読み出すこと

を特徴とする請求項 1 記載の暗号化装置。

【請求項 9】 上記公開鍵暗号化処理手段は、楕円曲線暗号化処理を行うことを特徴とする請求項 1 記載の暗号化装置。

【請求項 10】 上記ハッシュ値生成手段は、SHA-1 処理を行うことを特徴とする請求項 1 記載の暗号化装置。

【請求項 11】 通信機能を有する非接触型 IC カードに組み込まれているこ

と

を特徴とする請求項 1 記載の暗号化装置。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、いわゆる公開鍵暗号化方式による暗号化処理を行う暗号化装置に関する。

【0 0 0 2】

【従来の技術】

近年、例えば、いわゆるインターネット等を利用した電子商取引やオンラインショッピングといった各種通信技術を利用した様々なサービスが普及しつつある。また、近年では、通信技術の進歩にともない、端末を介した通信技術のみならず、例えば、交通機関の料金徴収やいわゆる電子マネー等に利用するための通信機能を集積回路化した非接触型半導体メモリカードといったカード状のデバイスも開発されている。

【0 0 0 3】

このような通信機能を有するカード状のデバイス（以下、非接触型 I C (Integrated Circuit) カードという。）は、取り扱いの便宜等の観点から、少ない回路規模で構成されるとともに、極めて少ない電力消費で動作するように構成される必要がある。

【0 0 0 4】

【発明が解決しようとする課題】

ところで、上述した非接触型 I C カードを用いたサービスにおいては、通常、通信相手の正当性を認証するための相互認証処理や、データ通信の安全性を確保するための暗号化処理が行われる。その際、非接触型 I C カードにおいては、処理の高速化が要求されることから、これらの機能をソフトウェアによって実装すると、高いクロックの C P U (Central Processing Unit) を要することとなり、実用的でない。そのため、非接触型 I C カードにおいては、これらの機能をソフトウェアによって実装するのではなく、ハードウェアによって実装するのが望

ましい。

【 0 0 0 5 】

ここで、このようなハードウェアによって上述した機能を実装する非接触型 I C カードにおいては、電力消費を極力抑制するために、例えばいわゆる D E S ( Data Encryption Standard ) 暗号化方式といった比較的少ない回路規模及び電力消費で実装することができるいわゆる共通鍵暗号化方式を採用するものが多かった。

【 0 0 0 6 】

しかしながら、暗号化及び復号に共通の鍵を用いる共通鍵暗号化方式は、鍵データの授受を行う必要があるといった観点から、不正な第三者による攻撃に弱いという問題がある。そのため、非接触型 I C カードにおいては、将来的に金融サービスに適用する場合等の問題が懸念されていた。

【 0 0 0 7 】

そのため、非接触型 I C カードを用いたサービスにおいては、非接触型 I C カードとして、例えばいわゆる R S A ( Rivest-Shamir-Adleman ) 暗号化方式や楕円曲線暗号化方式 ( Elliptic Curve Cryptosystem ; E C C ) といったように、暗号化と復号とに用いる鍵を異なるものとし、秘密に保つ必要がある共通鍵を特定の 1 人が持てばよいいわゆる公開鍵暗号化方式を採用したセキュリティの高いシステムが要求されつつあり、公開鍵を用いた署名生成及び署名検証を行う非接触型 I C カードの開発も多く試みられている。

【 0 0 0 8 】

しかしながら、公開鍵暗号化方式は、共通鍵暗号化方式に比べ、セキュリティ性が極めて向上するものの、演算量が非常に膨大となることから、これをハードウェアによって実装する際には、回路規模が数十倍に増大し、規模が増大した回路に供給する電力も必然的に増大することになる。

【 0 0 0 9 】

そのため、このような公開鍵暗号化方式を採用した非接触型 I C カードにおいては、回路規模、消費電力、及びコストの面で十分な特性を得ることができなかった。特に、非接触型 I C カードにおいては、限られた電力の多くを、暗号化処

理を行うための回路に供給する必要があることから、通信距離が数ミリ程度と短いものしか実用化されていないのが実情である。

【 0 0 1 0 】

このように、非接触型 I C カードにおいては、セキュリティの面で強固であり公開鍵暗号化方式を採用することが期待されているものの、供給可能な電力やチップサイズ等の制限があることから、実装することが極めて困難であった。

【 0 0 1 1 】

本発明は、このような実情に鑑みてなされたものであり、回路規模を削減し、極めて少ない電力消費のもとに高速且つ安全に公開鍵を用いた署名生成及び署名検証を可能とする暗号化装置を提供することを目的とする。

【 0 0 1 2 】

【課題を解決するための手段】

上述した目的を達成する本発明にかかる暗号化装置は、公開鍵暗号化方式による暗号化処理を行う暗号化装置であって、演算用の値を保持するためのレジスタ及び結果を取り込むためのレジスタからなるレジスタ群を有し、公開鍵暗号化方式による暗号化処理を行う公開鍵暗号化処理手段と、この公開鍵暗号化処理手段によって用いるハッシュ値を生成するハッシュ値生成手段とを備え、少なくとも、ハッシュ値生成手段における演算用の値を保持するためのレジスタ及び結果としてのハッシュ値を取り込むためのレジスタからなるレジスタ群を、公開鍵暗号化処理手段におけるレジスタ群と共用し、処理モードに応じて、動作させるハードウェアを時分割に切り替えることを特徴としている。

【 0 0 1 3 】

このような本発明にかかる暗号化装置は、公開鍵暗号化処理手段による暗号化処理とハッシュ値生成手段によるハッシュ値生成処理との間で、使用するレジスタ群を時分割共用する。

【 0 0 1 4 】

また、この本発明にかかる暗号化装置は、公開鍵暗号化処理手段によって暗号化処理を行う際に必要となる乱数を生成するために、共通鍵暗号化方式による暗号化処理を行う共通鍵暗号化処理手段を備え、この共通鍵暗号化処理手段におけ



るデータを保持するレジスタ及び鍵データを保持するレジスタからなるレジスタ群を、公開鍵暗号化処理手段におけるレジスタ群と共用することを特徴としている。

## 【 0 0 1 5 】

このような本発明にかかる暗号化装置は、共通鍵暗号化処理手段を備える場合には、公開鍵暗号化処理手段による暗号化処理とハッシュ値生成手段によるハッシュ値生成処理との間のみならず、この共通鍵暗号化処理手段による暗号化処理との間でも、使用するレジスタ群を時分割共用する。

## 【 0 0 1 6 】

さらに、この本発明にかかる暗号化装置において、公開鍵暗号化処理手段は、公開鍵暗号化方式による暗号化処理に際する各種演算処理を行う公開鍵暗号化演算処理コア手段を有し、ハッシュ値生成手段は、ハッシュ値の生成処理に際する各種演算処理を行うハッシュ値演算処理コア手段を有し、公開鍵暗号化演算処理コア手段と、ハッシュ値演算処理コア手段とを共用することを特徴としている。

## 【 0 0 1 7 】

このような本発明にかかる暗号化装置は、公開鍵暗号化処理手段による暗号化処理とハッシュ値生成手段によるハッシュ値生成処理との間で、演算処理に使用する演算処理コア手段を時分割共用する。

## 【 0 0 1 8 】

さらにまた、この本発明にかかる暗号化装置において、公開鍵暗号化処理手段は、ビット幅を可変とするためのバス切り替えスイッチを有し、ハッシュ値生成手段におけるバス切り替えスイッチを、公開鍵暗号化処理手段におけるバス切り替えスイッチと共用することを特徴としている。

## 【 0 0 1 9 】

このような本発明にかかる暗号化装置は、公開鍵暗号化処理手段による暗号化処理とハッシュ値生成手段によるハッシュ値生成処理との間で、バス切り替えスイッチを時分割共用する。

## 【 0 0 2 0 】

また、この本発明にかかる暗号化装置は、公開鍵暗号化処理手段によって暗号

化処理を行う際に必要となる乱数を生成するために、共通鍵暗号化方式による暗号化処理を行う共通鍵暗号化処理手段を備え、この共通鍵暗号化処理手段におけるバス切り替えスイッチを、公開鍵暗号化処理手段におけるバス切り替えスイッチと共用することを特徴としている。

#### 【 0 0 2 1 】

このような本発明にかかる暗号化装置は、共通鍵暗号化処理手段を備える場合には、公開鍵暗号化処理手段による暗号化処理とハッシュ値生成手段によるハッシュ値生成処理との間のみならず、この共通鍵暗号化処理手段による暗号化処理との間でも、バス切り替えスイッチを時分割共用する。

#### 【 0 0 2 2 】

さらに、この本発明にかかる暗号化装置は、ハッシュ値生成手段によって生成されたハッシュ値を格納する記憶手段を備え、ハッシュ値生成手段は、生成したハッシュ値を記憶手段に格納する際に、公開鍵暗号化処理手段によって用いられるアドレスに当該ハッシュ値を格納し、公開鍵暗号化処理手段は、記憶手段に格納されたハッシュ値を読み出すことを特徴としている。

#### 【 0 0 2 3 】

このような本発明にかかる暗号化装置は、ハッシュ値生成手段によって生成されたハッシュ値を、公開鍵暗号化処理手段による次回の暗号化処理にて用いるためにデータ転送することなく、記憶手段を介して受け渡す。

#### 【 0 0 2 4 】

##### 【発明の実施の形態】

以下、本発明を適用した具体的な実施の形態について図面を参照しながら詳細に説明する。

#### 【 0 0 2 5 】

この実施の形態は、例えば、通信機能を集積回路化した非接触型半導体メモリカードといったカード状のデバイス（以下、非接触型 I C (Integrated Circuit) カードという。）等に適用することができるものであって、通信相手の正当性を認証するための相互認証処理や、データ通信の安全性を確保するための暗号化処理の機能を、ハードウェアによって実装した暗号化装置である。特に、この暗

号化装置は、いわゆる公開鍵暗号化方式を採用するものであって、各種処理を行うための各ハードウェアを当該各種処理間で共用して時分割処理を行うことにより、回路規模を削減して極めて少ない電力消費のもとに高速且つ安全に公開鍵を用いた署名生成及び署名検証を可能とするものである。

【 0 0 2 6 】

なお、以下では、説明の便宜上、暗号化装置は、公開鍵暗号化方式として、いわゆる楕円曲線暗号化方式 (Elliptic Curve Cryptosystem ; ECC) を採用し、認証やデジタル署名等に用いるハッシュ関数として、いわゆる S H A - 1 (Secure Hash Algorithm-1) を用い、さらに、暗号化処理を行う際に必要となる鍵生成の過程等において用いる乱数を、共通鍵暗号化方式の 1 つであるいわゆる D E S (Data Encryption Standard) 暗号化方式を用いて生成するものとして説明する。すなわち、暗号化装置は、公開鍵暗号化方式の一連の信号処理として、少なくとも、これら楕円曲線暗号化処理、S H A - 1 処理、及び D E S 暗号化処理を行うものとして説明する。

【 0 0 2 7 】

まず、暗号化装置において、楕円曲線暗号化処理、S H A - 1 処理、及び D E S 暗号化処理を行うための各ハードウェアを共用するための概念について説明する。

【 0 0 2 8 】

まず、暗号化装置においては、楕円曲線暗号化処理、S H A - 1 処理、及び D E S 暗号化処理のそれぞれを行うためのハードウェア構成要素としてのレジスタを共用する。すなわち、楕円曲線暗号化処理を行う暗号化エンジンにおけるハードウェア構成要素は、機能分析的に分解すると、図 1 (A) に概念を示すように、レジスタ群と楕円曲線演算処理コア回路とに大別することができ、レジスタ群が当該ハードウェア構成要素の半分程度を占める。また、S H A - 1 処理を行う暗号化エンジンにおけるハードウェア構成要素についても、機能分析的に分解すると、同図 (B) に示すように、レジスタ群と S H A - 1 演算処理コア回路とに大別することができる。そこで、暗号化装置においては、同図 (C) に示すように、楕円曲線暗号化処理及び S H A - 1 処理のそれぞれを行うためのハードウェア

ア構成要素としてのレジスタを共用する。さらに、DES暗号化処理を行う暗号化エンジンにおけるハードウェア構成要素についても、機能分析的に分解すると、図示しないが、レジスタ群とDES演算処理コア回路とに大別することができることから、暗号化装置においては、楕円曲線暗号化処理及びSHA-1処理に加え、DES暗号化処理を行うためのハードウェア構成要素としてのレジスタをも共用する。これにより、暗号化装置は、回路規模の削減を図ることが可能となる。

## 【0029】

また、暗号化装置においては、SHA-1処理を行うための演算処理コア回路と楕円曲線暗号化処理を行う演算処理コア回路とを共用する。すなわち、ハッシュ値を算出するSHA-1処理においては、高速に動作する加算器が設けられた演算処理コア回路が必要とされる。また、楕円曲線暗号化処理においても、演算処理コア回路に加算器が設けられる。そこで、暗号化装置においては、SHA-1処理を行うための演算処理コア回路と楕円曲線暗号化処理を行う演算処理コア回路とにおける加算器等のゲート数が多いハードウェア構成要素を共用する。これにより、暗号化装置は、回路規模の削減を図ることが可能となる。

## 【0030】

さらに、暗号化装置においては、暗号化エンジンにおけるバス切り替えスイッチ群とその他各種機能の切り替えスイッチとを共用する。すなわち、公開鍵暗号化方式における鍵長を可変とするためにはバスを切り替える必要があることから、楕円曲線暗号化処理を行う暗号化エンジンには、例えば32ビット幅のスイッチが多数設けられる。これらのスイッチは、その構成上、SHA-1処理やDES暗号化処理を行うハードウェアにおいても共用可能である。そこで、暗号化装置においては、これらバス切り替えスイッチ群を、その他各種機能の切り替えスイッチとして流用する。これにより、暗号化装置は、回路規模の削減を図ることが可能となる。

## 【0031】

さらにまた、暗号化装置においては、レジスタやメモリ等のハードウェアを時分割共用する。すなわち、暗号化装置における公開鍵暗号化方式の信号処理は、

D E S 暗号化処理を用いた乱数の生成、S H A - 1 処理によるハッシュ値の算出、及び楕円曲線暗号化処理における楕円曲線の算出に大別される。しかしながら、これらの処理は、同時には行うことができないものであることから、ハードウェアを共用する場合には必然的に時分割処理を行うことになる。そこで、暗号化装置においては、これを利用して、レジスタやメモリ等のハードウェアを各処理で時分割共用する。これにより、暗号化装置は、回路規模の削減と電力消費の削減とを図ることが可能となる。

#### 【 0 0 3 2 】

このように、暗号化装置は、楕円曲線暗号化処理、S H A - 1 処理、及びD E S 暗号化処理を行うための各ハードウェアを共用し、時分割処理を行うものとして構成される。

#### 【 0 0 3 3 】

さて、暗号化装置においては、具体的に実装するにあたって、各ハードウェアを共用するために、楕円曲線暗号化処理、S H A - 1 処理、及びD E S 暗号化処理を行うための各ハードウェアを共用しやすい構成にする必要がある。以下では、これらの楕円曲線暗号化処理、S H A - 1 処理、及びD E S 暗号化処理を行うための各ハードウェアを共用しやすい構成とした具体的な実装例について説明した後、これらの各ハードウェアを統合した具体的な暗号化装置の実装例について説明する。

#### 【 0 0 3 4 】

まず、S H A - 1 処理を行うためのハードウェアであるS H A - 1 処理回路について説明する。

#### 【 0 0 3 5 】

S H A - 1 処理回路は、S H A - 1 処理を行うものである。S H A - 1 とは、認証やデジタル署名等に用いられるハッシュ関数の1つであり、512ビットの任意の原文から160ビットの擬似乱数であるハッシュ値を発生する不可逆な一方向性関数である。S H A - 1 は、原文が1ビットでも異なる場合には、全く異なるハッシュ値を出力することから、ハッシュ値を生成して通信経路の両端で比較することにより、通信途中で原文が改竄されたか否かを検出する用途に広く

用いられる。具体的には、SHA-1を用いたSHA-1処理においては、あるメッセージを送信する場合には、送信側がメッセージとこのメッセージに対するハッシュ値とを同時に送信し、受信側では受け取ったメッセージからハッシュ値を算出し、その結果得られたハッシュ値と送信側から送信されたハッシュ値とを比較することにより、データの改竄の有無を検証することができる。SHA-1処理回路は、このようなSHA-1処理を行うものとして構成されるが、ここでは、いわゆるFIPS (Federal Information Processing Standard) に規定されているSHA-1のうち、回路規模が比較的小さくて済む”ALTERNATIVE METHOD”を採用する。

#### 【0036】

この”ALTERNATIVE METHOD”のアルゴリズムは、通常であれば80個の32ビット・ワード配列 $W(0), \dots, W(79)$ を用いて行うSHA-1処理を少ないメモリ空間で実現するための代替手段であり、 $\{W(t)\}$ を循環キューとみなし、16個の32ビット・ワード配列 $W(0), \dots, W(15)$ を用いて行うものである。このアルゴリズムにおいては、512ビット長のブロック $M(i)$ 毎に、以下の4つの工程が行われる。なお、以下における値MASKは、16進数で0000000Fとする。

#### 【0037】

まず、このアルゴリズムにおいては、第1の工程として、ブロック $M(i)$ を16個のワード $W(0), \dots, W(15)$ に分割する。なお、ワード $W(0)$ は、最も左側のワードである。

#### 【0038】

続いて、このアルゴリズムにおいては、はじめの5つのワードバッファを、それぞれ、A, B, C, D, Eとし、次の5つのワードバッファを、それぞれ、H0, H1, H2, H3, H4とすると、第2の工程として、次式(1)に示す演算を行う。

#### 【0039】

【数 1】

$$\begin{cases} A = H0; \\ B = H1; \\ C = H2; \\ D = H3; \\ E = H4; \end{cases} \quad \dots (1)$$

【 0 0 4 0】

続いて、このアルゴリズムにおいては、第 3 の工程として、変数  $t$  を "0" から "7 9" まで変化させ、次式 (2) に示す演算を行う。

【 0 0 4 1】

【数 2】

$$\begin{cases} s = t \text{ AND } MASK; \\ \text{if } (t \geq 16) \\ W[s] = S1(W[(s+13) \text{ AND } MASK] \text{ XOR } W[(s+8) \text{ AND } MASK] \\ \quad \text{XOR } W[(s+2) \text{ AND } MASK] \text{ XOR } W[s]); \\ TEMP = S5(A) + F(t; B, C, D) + E + W[s] + Kt; \\ E = D; \\ D = C; \\ C = S30(B); \\ B = A; \\ A = TEMP; \end{cases} \quad \dots (2)$$

【 0 0 4 2】

なお、上式 (2) における  $S_n(X)$  は、 $X$  をワード値、 $n$  を  $0 \leq n < 32$  の整数としたときの循環左シフト操作を表すものである。また、上式 (2) における  $F(t; B, C, D)$  は、次式 (3) に示す関数であり、 $K(t)$  は、次式 (4) に示す 16 進数のワード定数列である。

【 0 0 4 3 】

【数 3】

$$\begin{cases} F(t; B, C, D) = (B \text{ AND } C) \text{ OR } ((\text{NOT } B) \text{ AND } D) & (0 \leq t \leq 19) \\ F(t; B, C, D) = B \text{ XOR } C \text{ XOR } D & (20 \leq t \leq 39) \\ F(t; B, C, D) = (B \text{ AND } C) \text{ OR } (B \text{ AND } D) \text{ OR } (C \text{ AND } D) & (40 \leq t \leq 59) \\ F(t; B, C, D) = B \text{ XOR } C \text{ XOR } D & (60 \leq t \leq 79) \end{cases} \quad \dots (3)$$

【 0 0 4 4 】

【数 4】

$$\begin{cases} K(t) = 5A827999 & (0 \leq t \leq 19) \\ K(t) = 6ED9EBA1 & (20 \leq t \leq 39) \\ K(t) = 8F1BBCDC & (40 \leq t \leq 59) \\ K(t) = CA62C1D6 & (60 \leq t \leq 79) \end{cases} \quad \dots (4)$$

【 0 0 4 5 】

そして、このアルゴリズムにおいては、第 4 の工程として、次式 (5) に示す演算を行い、一連の処理を終了する。

【 0 0 4 6 】

【数 5】

$$\begin{cases} H0 = H0 + A; \\ H1 = H1 + B; \\ H2 = H2 + C; \\ H3 = H3 + D; \\ H4 = H4 + E; \end{cases} \quad \dots (5)$$

【 0 0 4 7 】

ここで、このような "ALTERNATIVE METHOD" のアルゴリズムを一般的な形式で実



装すると、SHA-1 処理回路は、図 2 に示すような構成となる。

#### 【0048】

すなわち、SHA-1 処理回路は、同図に示すように、図示しない CPU (Central Processing Unit) から供給される演算用の値をテンポラリに保持するシフトレジスタ群 10 と、上述したワードバッファ A, B, C, D, E としての 5 つのシフトレジスタと上述した値 TEMP を保持するシフトレジスタとからなり結果としてのハッシュ値を取り込むためのシフトレジスタ群 20 と、初期値 H0, H1, H2, H3, H4 及び上式 (4) に示した 16 進数のワード定数列 K (t) を保持する ROM (Read Only Memory) 30 と、結果としてのハッシュ値を格納する ALU RAM (Arithmetic and Logical Unit Random Access Memory) 40 とを備えるとともに、上述したアルゴリズムにおける各種演算を行うための各種演算処理回路を備える。なお、同図における MUX0, MUX3, MUX4, MUX5 は、それぞれ、バス切り替えスイッチである。

#### 【0049】

ここで、SHA-1 処理回路においては、回路規模を考慮すると、上式 (2) 中、値 TEMP の算出式、すなわち、次式 (6) に示す演算を実行する 32 ビット 5 入力の加算器が最も回路規模の増大を招来する要因となる。そこで、SHA-1 処理回路としては、楕円曲線暗号化処理の演算時間に比べて SHA-1 処理の演算時間が無視できるほど短いことを利用して、図 3 に示すように、32 ビット 2 入力の加算器を 4 回用いることにより、回路規模を削減することが可能となる。

#### 【0050】

#### 【数 6】

$$TEMP = S5(A) + F(t; B, C, D) + E + W[s] + Kt; \quad \dots (6)$$

#### 【0051】

この場合、SHA-1 処理回路においては、図 2 に示した構成の場合に比べ、演算時間が約 4 ～ 5 倍程度になるものの、楕円曲線暗号化処理の演算時間に比べれば十分短時間であることから、実用上は何らの支障も招来せず、サイズが膨大

なデータやストリームに対して S H A - 1 処理を施すような特殊な場合を除けば、十分な性能を得ることが可能である。

【 0 0 5 2 】

なお、S H A - 1 処理回路においては、後述するように、楕円曲線暗号化処理の際に使用する加算器と兼用することにより、当該 S H A - 1 処理回路における加算器そのものが不要となることから、さらに大幅な回路規模の削減を図ることが可能となる。

【 0 0 5 3 】

また、S H A - 1 処理回路においては、上式 ( 2 ) 中、ワード  $W[s]$  の算出式、すなわち、次式 ( 7 ) に示す演算を実行する際に、必ず 3 2 ビット  $\times$  1 6 段のシフトレジスタが必要となることがわかる。

【 0 0 5 4 】

【数 7】

$$\begin{aligned} W[s] = & S1(W[(s+13) \text{ AND } MASK] \text{ XOR } W[(s+8) \text{ AND } MASK] \\ & \text{ XOR } W[(s+2) \text{ AND } MASK] \text{ XOR } W[s]); \\ & \dots (7) \end{aligned}$$

【 0 0 5 5 】

さらに、S H A - 1 処理回路においては、上式 ( 2 ) 中、ワードバッファ A, B, C, D, E の算出式、すなわち、次式 ( 8 ) に示す演算を実行する際にも、少なくとも 3 2 ビット  $\times$  5 ~ 6 段のシフトレジスタが必要となる。

【 0 0 5 6 】

【数 8】

$$\begin{cases} E = D; \\ D = C; \\ C = S30(B); \\ B = A; \\ A = TEMP; \end{cases} \dots (8)$$

【 0 0 5 7 】

ここで、楕円曲線暗号化処理を行うためのハードウェアである楕円曲線暗号化

処理回路においては、後述するように、段数が可変とされる32ビット×7段のシフトレジスタ群が3組設けられることから、SHA-1処理回路においては、これらのシフトレジスタを流用することにより、当該SHA-1処理回路に専用のシフトレジスタを設ける必要がなくなり、さらに大幅な回路規模の削減を図ることが可能となる。結果的に、暗号化装置においては、通常であれば60000ゲート以上からなるSHA-1処理回路を、楕円曲線暗号化処理回路に対して2000ゲート程度の追加回路のみで実現することができる。

## 【0058】

さて、このようなSHA-1処理回路は、図4及び図5に示すような一連の工程を経ることにより、基本動作を行う。なお、ここでは、先に図2に示した構成からなるSHA-1処理回路の基本動作について説明する。

## 【0059】

まず、SHA-1処理回路は、図4に示すように、ステップS1において、変数 $t$ を"0"とする。

## 【0060】

続いて、SHA-1処理回路は、ステップS2において、シフトレジスタ群10における各シフトレジスタに対して、パディングされたデータのうち、32×16ブロック(=512ビット)からなる先頭のデータをロードする。

## 【0061】

続いて、SHA-1処理回路は、ステップS3において、バス切り替えスイッチMUX0を、演算処理回路W[s]の出力側に切り替える。

## 【0062】

続いて、SHA-1処理回路は、ステップS4において、初期値H0, H1, H2, H3, H4をROM30から読み出し、バス切り替えスイッチMUX4、加算器、及びシフトレジスタ群20における値TEMPを保持するシフトレジスタを介して、シフトレジスタ群20におけるワードバッファA, B, C, D, Eとしての各シフトレジスタに対して順次ロードする。

## 【0063】

続いて、SHA-1処理回路は、ステップS5において、値TEMPとしてオ

ールゼロをセットする。

【0064】

続いて、SHA-1 処理回路は、ステップ S 6 において、バス切り替えスイッチ MUX 5 を制御して、次式 (9) に示すように、加算器によって 4 回に分けた加算処理を行うことにより、上式 (6) に示した演算と等価な演算を行い、値 TEMP を算出する。

【0065】

【数 9】

$$\begin{cases} SS(A) + F(t) \Rightarrow TEMP; \\ TEMP + E \Rightarrow TEMP; \\ TEMP + W[s] \Rightarrow TEMP; \\ TEMP + K(t) \Rightarrow TEMP; \end{cases} \quad \dots (9)$$

【0066】

続いて、SHA-1 処理回路は、ステップ S 7 において、バス切り替えスイッチ MUX 3 を、演算処理回路 S 3 0 の出力側に切り替え、各シフトレジスタに保持されている値 TEMP, A, B, C, D, E を、それぞれ、1 クロック分だけ右にシフトする。これにより、SHA-1 処理回路は、上式 (8) に示した各値を得ることができる。

【0067】

続いて、SHA-1 処理回路は、ステップ S 8 において、シフトレジスタ群 1 0 における各シフトレジスタに保持されている値を、それぞれ、1 クロック分だけ右にシフトする。

【0068】

続いて、SHA-1 処理回路は、ステップ S 9 において、変数 t が "79" に到達したか否かを判定する。ここで、SHA-1 処理回路は、変数 t が "79" に到達していないものと判定した場合には、ステップ S 1 0 へと処理を移行し、変数 t を "1" だけインクリメントした後、ステップ S 2 乃至ステップ S 8 の処理を繰り返す。すなわち、SHA-1 処理回路は、ステップ S 2 乃至ステップ S 8 の処理を、変数 t を "0" から "79" まで変化させて行う。

## 【 0 0 6 9 】

一方、SHA-1 処理回路は、変数  $t$  が "79" に到達したものと判定した場合には、ステップ S 1 1 へと処理を移行し、バス切り替えスイッチ MUX 3 を、演算処理回路 S 3 0 の出力側とは反対側に切り替えるとともに、バス切り替えスイッチ MUX 4 を、ROM 3 0 の出力側に切り替え、さらに、バス切り替えスイッチ MUX 5 の出力をワードバッファ E としてのシフトレジスタからの出力とすることにより、ワードバッファ A, B, C, D, E としての各シフトレジスタに保持されている値に対して、それぞれ、初期値 H 0, H 1, H 2, H 3, H 4 を加算器によって加算する。

## 【 0 0 7 0 】

続いて、SHA-1 処理回路は、ステップ S 1 1 における加算器による演算結果が、値 TEMP を保持するシフトレジスタに供給されることから、ステップ S 1 2 において、上式 (5) の演算を実現するように、各シフトレジスタに保持されている値を、それぞれ、6 クロック分だけ右にシフトする。

## 【 0 0 7 1 】

そして、SHA-1 処理回路は、図 5 に示すように、ステップ S 1 3 において、ワードバッファ A, B, C, D, E としての各シフトレジスタに保持されている値を、それぞれ、ALU RAM 4 0 に格納する。

## 【 0 0 7 2 】

続いて、SHA-1 処理回路は、ステップ S 1 4 において、パディングの結果が 5 1 2 ビットであるか否かを判定する。

## 【 0 0 7 3 】

ここで、SHA-1 処理回路は、パディングの結果が 5 1 2 ビットであるものと判定した場合には、ステップ S 1 3 において ALU RAM 4 0 に格納された値が、最終的なハッシュ値となることから、そのまま一連の処理を終了する。

## 【 0 0 7 4 】

一方、SHA-1 処理回路は、パディングの結果が 5 1 2 ビットでない、すなわち、5 1 2 ビットを超えるものと判定した場合には、ステップ S 1 5 において、パディングしたデータが全てシフトレジスタ群 1 0 における各シフトレジスタ

に対してロードされて処理が終了したか否かを判定する。

【0075】

ここで、SHA-1 処理回路は、パディングしたデータが全てシフトレジスタ群 10 における各シフトレジスタに対してロードされておらず処理が終了していないものと判定した場合には、ステップ S 16 において、ステップ S 13 における状態を保持しつつ、次の 512 ビットのデータをシフトレジスタ群 10 における各シフトレジスタに対してロードする。

【0076】

続いて、SHA-1 処理回路は、ステップ S 17 において、バス切り替えスイッチ MUX 4 を、ALU RAM 40 の出力側に切り替え、ステップ S 13 において ALU RAM 40 に格納された値を、それぞれ、ワードバッファ A, B, C, D, E としての各シフトレジスタに対してロードする。

【0077】

続いて、SHA-1 処理回路は、ステップ S 18 において、バス切り替えスイッチ MUX 0 を、演算処理回路 W[s] の出力側に切り替え、図 4 中ステップ S 5 からの処理を繰り返す。

【0078】

そして、SHA-1 処理回路は、ステップ S 15 における判定の結果、パディングしたデータが全てシフトレジスタ群 10 における各シフトレジスタに対してロードされて処理が終了したものと判定した場合には、ステップ S 13 において ALU RAM 40 に格納された値が、最終的なハッシュ値となることから、そのまま一連の処理を終了する。

【0079】

SHA-1 処理回路は、このような一連の処理を行うことにより、ハッシュ値を生成する。

【0080】

つぎに、楕円曲線暗号化処理を行うためのハードウェアである楕円曲線暗号化処理回路について説明する。

【0081】

楕円曲線暗号化処理回路は、楕円曲線暗号化処理を行うものである。楕円曲線暗号化とは、暗号化と復号とに異なる通信鍵を用いる公開鍵暗号化アルゴリズムの1つであり、160ビット長の鍵を用いることにより、1024ビット長の鍵を用いたいわゆるRSA (Rivest-Shamir-Adleman) 暗号化方式と同等の性能を発揮する暗号化方式である。暗号化装置において、楕円曲線暗号化処理回路は、いわゆるモンゴメリー (Montgomery) 法を用いて構成される。すなわち、楕円曲線暗号化処理回路は、図6に示すように、図示しないCPUから供給される演算用の値をテンポラリに保持する32ビット幅のシフトレジスタ群50、60と、結果を取り込むためのシフトレジスタ群70と、主に32ビット幅の入力を有する図示しない加算器、減算器、及び乗算器を内部に有する楕円曲線演算処理コア回路80とを備える。なお、同図におけるMUX0、MUX1、MUX2は、それぞれ、バス切り替えスイッチである。

#### 【0082】

このような楕円曲線暗号化処理回路においては、モンゴメリー法と称される特殊な手法を用いて処理の高速化及び回路規模の削減を実現する。モンゴメリー法による楕円曲線演算処理コア回路80は、主に、加算器、減算器、及び乗算器の組み合わせ回路によって構成され、演算のステップ毎に32ビット幅のデータ同士の処理を行う。そこで、暗号化装置においては、回路規模の削減を図るために、上述したように、楕円曲線演算処理コア回路80の内部に設けられる加算器を、SHA-1処理回路における加算器と共用する。

#### 【0083】

また、楕円曲線暗号化処理回路においては、3組の32ビット幅のシフトレジスタ群50、60、70が設けられるが、例えば160ビット幅、192ビット幅、又は224ビット幅にも対応するために、各シフトレジスタ群50、60、70のそれぞれに対応して、ビット幅を可変とするためのバス切り替えスイッチMUX0、MUX1、MUX2が設けられる。すなわち、楕円曲線暗号化処理回路においては、160ビット幅、192ビット幅、又は224ビット幅にも対応するために、3組の32ビット幅のシフトレジスタ群50、60、70が、それぞれ、5、6、7段に切り替え可能に構成される。

## 【 0 0 8 4 】

この具体例としては、図 7 (A) にシフトレジスタ群 6 0 の近傍の要部構成を示すように、入力と、5 段目、6 段目、及び 7 段目のシフトレジスタのそれぞれからの出力とのうち、いずれか 1 つの信号を、バス切り替えスイッチ MUX 1 からの出力とするように、シフトレジスタ群 6 0 における各シフトレジスタのうち、右側のシフトレジスタから個数を可変とするものが考えられる。また、他の具体例としては、図 7 (B) にシフトレジスタ群 6 0 の近傍の要部構成を示すように、入力と、7 段目のシフトレジスタのそれぞれからの出力とのうち、いずれか 1 つの信号を出力とするバス切り替えスイッチ MUX 1 を設けるとともに、1 段目のシフトレジスタの後段にバス切り替えスイッチ MUX 2 を設け、さらに、2 段目のシフトレジスタの後段にバス切り替えスイッチ MUX 3 を設けるといったように、シフトレジスタ群 6 0 における各シフトレジスタのうち、左側のシフトレジスタから個数を可変とするものが考えられる。なお、楕円曲線暗号化処理回路においては、シフトレジスタ群 5 0, 7 0 についても、同様に構成することができる。

## 【 0 0 8 5 】

このように、楕円曲線暗号化処理回路においては、3 組の 3 2 ビット幅のシフトレジスタ群 5 0, 6 0, 7 0 のそれぞれに対応して、ビット幅を可変とするためのバス切り替えスイッチ MUX 0, MUX 1, MUX 2 が設けられる。そこで、暗号化装置においては、回路規模の削減を図るために、上述したように、楕円曲線暗号化処理回路におけるシフトレジスタ群 5 0, 6 0, 7 0 と、SHA-1 処理回路におけるシフトレジスタとを共用するとともに、楕円曲線暗号化処理回路におけるバス切り替えスイッチ MUX 0, MUX 1, MUX 2 と、SHA-1 処理回路におけるバス切り替えスイッチとを共用する。

## 【 0 0 8 6 】

さらに、上述した SHA-1 処理回路は、先に図 3 に示したように構成すると、3 2 ビット幅のシフトレジスタ群を用いて構成することができる。このような SHA-1 処理回路において、最終的な結果としてのハッシュ値や演算途中経過の値を保持するシフトレジスタは、先に図 2 に示したように、ALU RAM に



代替することができる。したがって、暗号化装置においては、楕円曲線暗号化処理回路における演算処理で用いる図示しないALU RAMとSHA-1処理回路におけるALU RAMとを共用する。これにより、暗号化装置においては、回路規模を抑制するのみならず、次の楕円曲線暗号化処理にて用いるハッシュ値をALU RAMに即座に格納することから、データ転送の手間を省略し、処理の高速化を図ることも可能となる。

【0087】

最後に、DES暗号化処理を行うためのハードウェアであるDES暗号化処理回路について説明する。

【0088】

DES暗号化処理回路は、DES暗号化処理を行うものである。DES暗号化とは、暗号化と復号とに同じ通信鍵を用いる共通鍵暗号化アルゴリズムの1つである。暗号化装置において、DES暗号化処理回路は、DES暗号化処理を3重に行ういわゆるトリプルDES暗号化処理を行うものとして構成される。

【0089】

ここで、DES暗号化処理回路においては、トリプルDES暗号化処理を行うことから、通常のシングルDES暗号化処理を行う場合に比べ、鍵データを保持するシフトレジスタ群の規模が大きくなり、ビット列に対してDES暗号化処理を施す際の連鎖技法であるいわゆるCBC (Cipher Block Chaining) モードを行う際にも、シフトレジスタ群が必要となる。したがって、DES暗号化処理回路においては、これらのシフトレジスタ群をゲート換算すると、いわゆるSボックスに比較しても大きく、全体として回路規模を増大させる要因となる。

【0090】

ところで、トリプルDES暗号化処理は、1つのDES演算処理コア回路を用いて、鍵データを3種類に変化させて3回演算処理を行うことによって実行される。そこで、DES暗号化処理回路としては、いわゆるType Aの非接触型ICカードに適用する場合には、先に図6に示した楕円曲線暗号化処理回路におけるシフトレジスタ群70を、この鍵データを保持するシフトレジスタ群として用いれば、楕円曲線暗号化処理回路に対する追加回路として、64ビット幅又は

32ビット幅のバス切り替えスイッチを1つだけ設けるだけでよい。ここで、バス切り替えスイッチは、楕円曲線暗号化処理回路にも設けられていることから、DES暗号化処理回路としては、このバス切り替えスイッチを流用すれば追加回路も不要となる。一方、DES暗号化処理回路としては、いわゆるType Bの非接触型ICカードに適用する場合には、予め3種類の鍵データを用意しておき、シングルDES暗号化処理を行う毎に、2個のシフトレジスタ分だけシフトして鍵データを交換することにより、Type Aの場合と同様な動作を行うことができる。また、DES暗号化処理回路においては、データを保持するシフトレジスタや結果を保持するシフトレジスタについても、楕円曲線暗号化処理回路におけるシフトレジスタ群と共用することができることから、非常に僅かな追加回路でトリプルDES暗号化処理を行うことが可能となる。

#### 【0091】

このようなDES暗号化処理回路は、具体的には、図8に示すように構成することができる。すなわち、DES暗号化処理回路は、図示しないCPUから供給されるデータを保持する32ビット幅のシフトレジスタ群90と、鍵データを保持するシフトレジスタ群100と、DES演算処理コア回路120を有する演算処理回路110とを備える。なお、同図におけるMUX、MUX0は、それぞれ、バス切り替えスイッチである。

#### 【0092】

DES暗号化処理回路においては、本来であれば64ビット幅のバッファを必要とするところ、32ビット幅のシフトレジスタ群90、100でまかなうことができる。また、DES暗号化処理回路においては、トリプルDES暗号化処理に用いる鍵データの交換を行うためにバス切り替えスイッチを用いず、巡回させる形式とすることにより、バス切り替えスイッチを不要としている。このように、DES暗号化処理回路は、上述した楕円曲線暗号化処理回路に対して、DES演算処理コア回路120を含む演算処理回路110以外には殆ど追加回路を必要とせず、大幅に回路規模を削減することが可能となる。

#### 【0093】

さて、以上では、各部を共用しやすい構成としたSHA-1処理回路、楕円曲

線暗号化処理回路、及びDES暗号化処理回路について説明したが、以下では、これらのSHA-1処理回路、楕円曲線暗号化処理回路、及びDES暗号化処理回路を統合して暗号化装置を構成することを考える。

#### 【0094】

先に図2に示したSHA-1処理回路、図6に示した楕円曲線暗号化処理回路、及び図8に示したDES暗号化処理回路を、それぞれ、重ね合わせると、共通の構成部位が極めて多く存在することがわかる。したがって、暗号化装置は、図9に示すように構成することができる。

#### 【0095】

すなわち、暗号化装置は、同図に示すように、2つのシフトレジスタ群200、210と、先に図2に示したSHA-1処理回路におけるROM30に相当するROM220と、先に図2に示したSHA-1処理回路におけるALU RAM40及び先に図6に示した楕円曲線暗号化処理回路における楕円曲線演算処理コア回路80として機能するモンゴメリー演算回路230と、先に図8に示したDES暗号化処理回路における演算処理回路110に相当する演算処理回路240と、SHA-1処理における各種演算を行うための上述した各種演算処理回路とを備える。なお、同図においては、シフトレジスタ群200と演算処理回路240との配線については図示を省略している。

#### 【0096】

より具体的には、暗号化装置においては、先に図2に示したSHA-1処理回路におけるシフトレジスタ群10と、先に図6に示した楕円曲線暗号化処理回路におけるシフトレジスタ群50、60と、先に図8に示したDES暗号化処理回路におけるシフトレジスタ群90、100とを、シフトレジスタ群200として共用する。また、暗号化装置においては、先に図2に示したSHA-1処理回路におけるシフトレジスタ群20と、先に図6に示した楕円曲線暗号化処理回路におけるシフトレジスタ群70とを、シフトレジスタ群210として共用する。

#### 【0097】

さらに、暗号化装置においては、モンゴメリー演算回路230とSHA-1処理にて用いられる加算器とを、バス切り替えスイッチMUXを介して接続するこ

とにより、楕円曲線暗号化処理にて用いられる加算器を削減している。

【 0 0 9 8 】

さらにまた、暗号化装置においては、先に図 2 に示した S H A - 1 処理回路におけるバス切り替えスイッチ M U X 0 と、先に図 6 に示した楕円曲線暗号化処理回路におけるバス切り替えスイッチ M U X 0 と、先に図 8 に示した D E S 暗号化処理回路におけるバス切り替えスイッチ M U X 0 とを共用するとともに、先に図 6 に示した楕円曲線暗号化処理回路におけるバス切り替えスイッチ M U X 1 と、先に図 8 に示した D E S 暗号化処理回路におけるバス切り替えスイッチ M U X 0 とを共用する。

【 0 0 9 9 】

このように、暗号化装置においては、S H A - 1 処理回路、楕円曲線暗号化処理回路、及び D E S 暗号化処理回路における各部を共用することができ、後述する各処理モードに応じて動作させるハードウェアを時分割に切り替えることにより、本来必要とされるゲート数の約 1 / 2 程度のゲート数にまで回路規模を削減することができる。また、暗号化装置においては、回路規模の削減にともない、消費電力も約 1 / 2 程度にまで削減することができる。

【 0 1 0 0 】

さらに、暗号化装置においては、これらの各部を制御する図示しない C P U の負荷も削減することができる。例えば、暗号化装置においては、S H A - 1 処理によって算出されたハッシュ値の A L U    R A M 上における格納場所を、楕円曲線暗号化処理にて用いられるアドレスに予め設定しておくことにより、S H A - 1 処理によるハッシュ値の算出後に、そのまま楕円曲線暗号化処理へと即座に移行することができることから、署名生成及び署名検証等の一連の動作の大半をハードウェアによって高速に実行することができる。したがって、暗号化装置においては、C P U の負荷を削減することができ、さらには、ソフトウェアの改竄等による攻撃に対する耐性も強固となる。通常、暗号化処理においては、途中の演算結果の授受を C P U に委任した場合には、ソフトウェアを改竄することによって容易に成りすましを許容してしまう一方で、暗号化装置においては、このような演算途中における C P U の介入による改竄を回避することができる。

## 【 0 1 0 1 】

さて、以下では、このような暗号化装置を適用した応用例について説明する。

## 【 0 1 0 2 】

暗号化装置は、上述したように、非接触型 I C カードに適用することができる。

## 【 0 1 0 3 】

非接触 I C カードは、例えば図 1 0 に示すように、各部を制御する C P U 3 0 0 と、この C P U 3 0 0 のワークエリアとして機能するメモリであって例えば 2 K B 程度の容量を有する R A M 3 1 0 と、各種プログラム等を記憶する読み出し専用のメモリであって例えば 3 2 K B 程度の容量を有する R O M 3 2 0 と、電氣的に書き換え可能とされるメモリであって例えば 9 K B 程度の容量を有する E E P R O M (Electrically Erasable Programmable Read Only Memory) 3 3 0 と、電源回路等のアナログブロック 3 4 0 と、無線通信を行うための R F (Radio Frequency) ブロック 3 5 0 と、上述した楕円曲線暗号化処理、S H A - 1 処理、及びトリプル D E S 暗号化処理を行う暗号化装置に相当する E C C / S H A 1 / D E S ブロック 3 6 0 と、例えば 1 K B 程度の容量を有する上述した A L U R A M 3 7 0 と、テスター用のランドからなるテストブロック 3 8 0 と、C P U 3 0 0 と各部との間でデータの授受を行うためのバスである C P U インターフェース 3 9 0 とを集積回路化したいわゆる L S I (Large Scale Integration) として構成される。

## 【 0 1 0 4 】

このような非接触型 I C カードは、先に図 9 に示した暗号化装置が E C C / S H A 1 / D E S ブロック 3 6 0 として組み込まれたものである。非接触 I C カードは、C P U 3 0 0 の制御のもとに、E C C / S H A 1 / D E S ブロック 3 6 0 を動作させ、楕円曲線暗号化処理、S H A - 1 処理、及びトリプル D E S 暗号化処理を行う。このとき、非接触型 I C カードは、上述したように、各処理モードに応じて、動作させるハードウェアを時分割に切り替える。

## 【 0 1 0 5 】

この時分割動作を具体的に説明するために、図 1 1 に示すように、各部を機能

的に表現する。なお、同図においては、アナログブロック 3 4 0 については図示を省略するとともに、説明の便宜上、ECC/SHA1/DES ブロック 3 6 0 を、楕円曲線暗号化処理及び SHA-1 処理の機能を表す ECC/SHA1 ブロック 3 6 0<sub>1</sub> と、トリプル DES 暗号化処理の機能を表す DES ブロック 3 6 0<sub>2</sub> とに大別して表現している。

## 【 0 1 0 6 】

このような非接触型 IC カードにおける処理モードは、主に、通信を行う通信モード、楕円曲線暗号化処理を行う楕円曲線暗号化処理モード、トリプル DES 暗号化処理を行う DES 暗号化処理モード、及び ALU RAM 3 7 0 に対してアクセスする ALU RAM モードの 4 つに大別される。

## 【 0 1 0 7 】

非接触型 IC カードにおいては、通信モード時には、図 1 2 (A) 中太線枠で示すように、CPU 3 0 0、RAM 3 1 0、ROM 3 2 0、EEPROM 3 3 0、及び RF ブロック 3 5 0 が動作する。すなわち、非接触型 IC カードにおいては、通信モード時には、CPU 3 0 0 の制御のもとに、ROM 3 2 0 に記憶されている所定の通信プログラムが起動し、RAM 3 2 0 や EEPROM 3 3 0 に記憶されている各種情報が、RF ブロック 3 5 0 を介して外部に送信されるとともに、RF ブロック 3 5 0 を介して外部から受信した各種情報が、RAM 3 2 0 や EEPROM 3 3 0 に記憶される。

## 【 0 1 0 8 】

また、非接触型 IC カードにおいては、楕円曲線暗号化処理モード時には、同図 (B) 中太線枠で示すように、ECC/SHA1 ブロック 3 6 0<sub>1</sub> 及び ALU RAM 3 7 0 が動作する。すなわち、非接触型 IC カードにおいては、楕円曲線暗号化処理モード時には、ECC/SHA1 ブロック 3 6 0<sub>1</sub> によって SHA-1 処理が行われ、得られたハッシュ値が ALU RAM 3 7 0 に格納されるとともに、このハッシュ値が ALU RAM 3 7 0 から読み出され、このハッシュ値を用いて ECC/SHA1 ブロック 3 6 0<sub>1</sub> によって楕円曲線暗号化処理が行われる。

## 【 0 1 0 9 】

さらに、非接触型 I C カードにおいては、D E S 暗号化処理モード時には、同図 (C) 中太線枠で示すように、C P U 3 0 0、R A M 3 1 0、R O M 3 2 0、及び D E S ブロック 3 6 0<sub>2</sub> が動作する。すなわち、非接触型 I C カードにおいては、D E S 暗号化処理モード時には、C P U 3 0 0 の制御のもとに、R O M 3 2 0 に記憶されている所定の擬似乱数 (Pseudo-random Number ; 以下、P N という。) 系列がシード (seed) や鍵データとして読み出され、R A M 3 1 0 がワークエリアとして用いられながら、D E S ブロック 3 6 0<sub>2</sub> によってトリプル D E S 暗号化処理が行われる。

#### 【 0 1 1 0 】

さらにまた、非接触型 I C カードにおいては、A L U R A M モード時には、同図 (D) 中太線枠で示すように、C P U 3 0 0、R A M 3 1 0、R O M 3 2 0、及び A L U R A M 3 7 0 が動作する。すなわち、非接触型 I C カードにおいては、A L U R A M モード時には、C P U 3 0 0 の制御のもとに、R O M 3 2 0 に記憶されている所定の各種情報が読み出され、R A M 3 1 0 がワークエリアとして用いられながら、A L U R A M 3 7 0 に対するアクセスが行われる。

#### 【 0 1 1 1 】

このように、非接触型 I C カードにおいては、各処理モードに応じて、動作させるハードウェアを時分割に切り替えることにより、ハードウェアを共用した構成であっても、同時には行うことができない複数の処理を行うことが可能となり、回路規模の削減と電力消費の削減とを図ることができる。

#### 【 0 1 1 2 】

以上説明したように、本発明の実施の形態として示す暗号化装置は、各種処理を行うための各ハードウェアを当該各種処理間で共用して時分割処理を行うことにより、回路規模を削減して極めて少ない電力消費のもとに高速且つ安全に公開鍵を用いた署名生成及び署名検証を行うことができる。

#### 【 0 1 1 3 】

したがって、暗号化装置は、L S I 等として実装する際に、チップサイズを大幅に小型化することができることから、非接触型 I C カード等にも容易に適用することができる。このとき、暗号化装置は、電力消費が少なくて済むことから、

非接触型 I C カードに適用した場合であっても、数センチメートルもの実用的な通信距離を実現することができる。また、暗号化装置は、改竄等の攻撃に対する耐性にも優れていることから、高い安全性が要求される非接触型 I C カードを用いたサービスに適用して有効である。

【 0 1 1 4 】

なお、本発明は、上述した実施の形態に限定されるものではない。例えば、上述した実施の形態では、公開鍵暗号化方式として、楕円曲線暗号化方式を採用して説明したが、本発明は、例えば R S A 暗号化方式等の他の公開鍵暗号化方式にも容易に適用することができる。

【 0 1 1 5 】

また、上述した実施の形態では、ハッシュ関数として、S H A - 1 を用いるものとして説明したが、本発明は、例えば M D 5 (Message Digest 5) 等の他のハッシュ関数にも容易に適用することができる。

【 0 1 1 6 】

さらに、上述した実施の形態では、暗号化処理を行う際に必要となる鍵生成の過程等において用いる乱数を、共通鍵暗号化方式の 1 つである D E S 暗号化方式を用いて生成するものとして説明したが、本発明は、乱数生成の手法については、任意のものを適用することができる。

【 0 1 1 7 】

さらにまた、上述した実施の形態では、暗号化装置の適用例として、非接触型 I C カードを用いて説明したが、本発明は、同様の機能を要求する任意の装置やデバイスに適用することができるのは勿論である。

【 0 1 1 8 】

このように、本発明は、その趣旨を逸脱しない範囲で適宜変更が可能であることとはいうまでもない。

【 0 1 1 9 】

【発明の効果】

以上詳細に説明したように、本発明にかかる暗号化装置は、公開鍵暗号化方式による暗号化処理を行う暗号化装置であって、演算用の値を保持するためのレジ



スタ及び結果を取り込むためのレジスタからなるレジスタ群を有し、公開鍵暗号化方式による暗号化処理を行う公開鍵暗号化処理手段と、この公開鍵暗号化処理手段によって用いるハッシュ値を生成するハッシュ値生成手段とを備え、少なくとも、ハッシュ値生成手段における演算用の値を保持するためのレジスタ及び結果としてのハッシュ値を取り込むためのレジスタからなるレジスタ群を、公開鍵暗号化処理手段におけるレジスタ群と共用し、処理モードに応じて、動作させるハードウェアを時分割に切り替える。

#### 【0120】

したがって、本発明にかかる暗号化装置は、公開鍵暗号化処理手段による暗号化処理とハッシュ値生成手段によるハッシュ値生成処理との間で、使用するレジスタ群を時分割共用することにより、回路規模を削減して極めて少ない電力消費のもとに公開鍵を用いた署名生成及び署名検証を安全に行うことができる。

#### 【0121】

また、この本発明にかかる暗号化装置は、公開鍵暗号化処理手段によって暗号化処理を行う際に必要となる乱数を生成するために、共通鍵暗号化方式による暗号化処理を行う共通鍵暗号化処理手段を備え、この共通鍵暗号化処理手段におけるデータを保持するレジスタ及び鍵データを保持するレジスタからなるレジスタ群を、公開鍵暗号化処理手段におけるレジスタ群と共用する。

#### 【0122】

したがって、本発明にかかる暗号化装置は、共通鍵暗号化処理手段を備える場合には、公開鍵暗号化処理手段による暗号化処理とハッシュ値生成手段によるハッシュ値生成処理との間のみならず、この共通鍵暗号化処理手段による暗号化処理との間でも、使用するレジスタ群を時分割共用することにより、より回路規模と電力消費とを削減することができる。

#### 【0123】

さらに、この本発明にかかる暗号化装置において、公開鍵暗号化処理手段は、公開鍵暗号化方式による暗号化処理に際する各種演算処理を行う公開鍵暗号化演算処理コア手段を有し、ハッシュ値生成手段は、ハッシュ値の生成処理に際する各種演算処理を行うハッシュ値演算処理コア手段を有し、公開鍵暗号化演算処理

コア手段と、ハッシュ値演算処理コア手段とを共用する。

【 0 1 2 4 】

さらにまた、この本発明にかかる暗号化装置において、公開鍵暗号化処理手段は、ビット幅を可変とするためのバス切り替えスイッチを有し、ハッシュ値生成手段におけるバス切り替えスイッチを、公開鍵暗号化処理手段におけるバス切り替えスイッチと共用する。

【 0 1 2 5 】

したがって、本発明にかかる暗号化装置は、公開鍵暗号化処理手段による暗号化処理とハッシュ値生成手段によるハッシュ値生成処理との間で、演算処理に使用する演算処理コア手段を時分割共用し、また、公開鍵暗号化処理手段による暗号化処理とハッシュ値生成手段によるハッシュ値生成処理との間で、バス切り替えスイッチを時分割共用することにより、さらに大幅な回路規模の削減と電力消費の削減とを図ることができる。

【 0 1 2 6 】

また、この本発明にかかる暗号化装置は、公開鍵暗号化処理手段によって暗号化処理を行う際に必要となる乱数を生成するために、共通鍵暗号化方式による暗号化処理を行う共通鍵暗号化処理手段を備え、この共通鍵暗号化処理手段におけるバス切り替えスイッチを、公開鍵暗号化処理手段におけるバス切り替えスイッチと共用する。

【 0 1 2 7 】

したがって、本発明にかかる暗号化装置は、共通鍵暗号化処理手段を備える場合には、公開鍵暗号化処理手段による暗号化処理とハッシュ値生成手段によるハッシュ値生成処理との間のみならず、この共通鍵暗号化処理手段による暗号化処理との間でも、バス切り替えスイッチを時分割共用することにより、より回路規模と電力消費とを削減することができる。

【 0 1 2 8 】

さらに、この本発明にかかる暗号化装置は、ハッシュ値生成手段によって生成されたハッシュ値を格納する記憶手段を備え、ハッシュ値生成手段は、生成したハッシュ値を記憶手段に格納する際に、公開鍵暗号化処理手段によって用いられ

るアドレスに当該ハッシュ値を格納し、公開鍵暗号化処理手段は、記憶手段に格納されたハッシュ値を読み出す。

【0129】

したがって、本発明にかかる暗号化装置は、ハッシュ値生成手段によって生成されたハッシュ値を、公開鍵暗号化処理手段による次回の暗号化処理にて用いるためにデータ転送することなく、記憶手段を介して受け渡すことにより、回路規模及び電力消費の削減のみならず、処理の高速化も図ることができる。

【図面の簡単な説明】

【図1】

本発明の実施の形態として示す暗号化装置の概念を説明する図であって、(A)は、楕円曲線暗号化処理を行う暗号化エンジンにおけるハードウェア構成要素を機能分析的に分解した様子を示し、(B)は、SHA-1処理を行う暗号化エンジンにおけるハードウェア構成要素を機能分析的に分解した様子を示し、(C)は、楕円曲線暗号化処理及びSHA-1処理のそれぞれを行うためのハードウェア構成要素としてのレジスタを共用した様子を示す図である。

【図2】

SHA-1処理回路の具体的な実装例としての構成を説明するブロック図である。

【図3】

SHA-1処理回路の具体的な実装例としての他の構成を説明するブロック図である。

【図4】

図2に示すSHA-1処理回路における基本動作を説明するためのフローチャートである。

【図5】

図2に示すSHA-1処理回路における基本動作を説明するためのフローチャートであって、図4に示す工程に続く残りの工程を説明する図である。

【図6】

楕円曲線暗号化処理回路の具体的な実装例としての構成を説明するブロック図

である。

【図 7】

同楕円曲線暗号化処理回路の具体的な実装例としての要部構成を説明するブロック図であって、(A)は、シフトレジスタ群における各シフトレジスタのうち、右側のシフトレジスタから個数を可変としてビット幅を切り替える場合の構成を示し、(B)は、シフトレジスタ群における各シフトレジスタのうち、左側のシフトレジスタから個数を可変としてビット幅を切り替える場合の構成を示す図である。

【図 8】

DES暗号化処理回路の具体的な実装例としての構成を説明するブロック図である。

【図 9】

同暗号化装置の具体的な実装例としての構成を説明するブロック図である。

【図 10】

同暗号化装置を適用した非接触型 IC カードの構成を説明するブロック図である。

【図 11】

同非接触型 IC カードにおける各部を機能的に表現したブロック図である。

【図 12】

同非接触型 IC カードにおける時分割動作を説明するための図であり、(A)は、通信モード時における動作を説明するためのブロック図であり、(B)は、楕円曲線暗号化処理モード時における動作を説明するためのブロック図であり、(C)は、DES暗号化処理モード時における動作を説明するためのブロック図であり、(D)は、ALU RAMモード時における動作を説明するためのブロック図である。

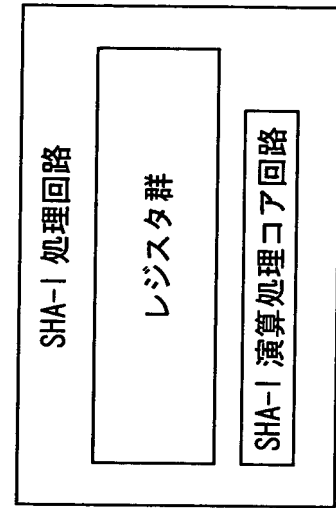
【符号の説明】

10, 20, 50, 60, 70, 90, 100, 200, 210 シフトレジスタ群、 30, 220, 320 ROM、 40, 370 ALU RAM、 80 楕円曲線演算処理コア回路、 110 演算処理回路、 120 DE

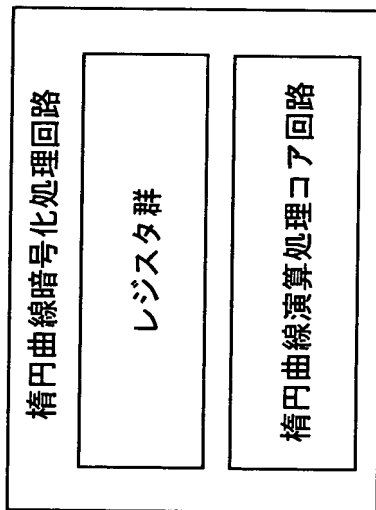
S演算処理コア回路、 230 モンゴメリー演算回路、 300 CPU、  
310 RAM、 330 EEPROM、 340 アナログブロック、 3  
50 RFブロック、 360 ECC/SHA1/DESブロック、 360  
1 ECC/SHA1ブロック、 360<sub>2</sub> DESブロック、 380 テス  
トブロック、 390 CPUインターフェース

【書類名】 図面

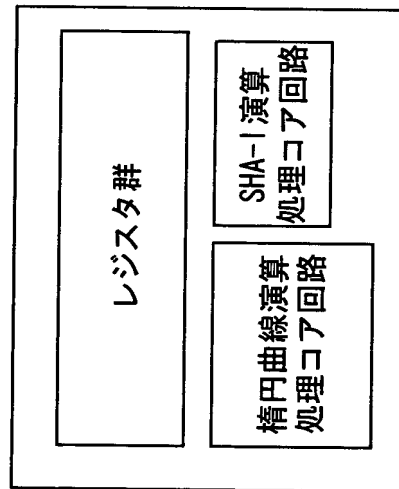
【図 1】



(B)



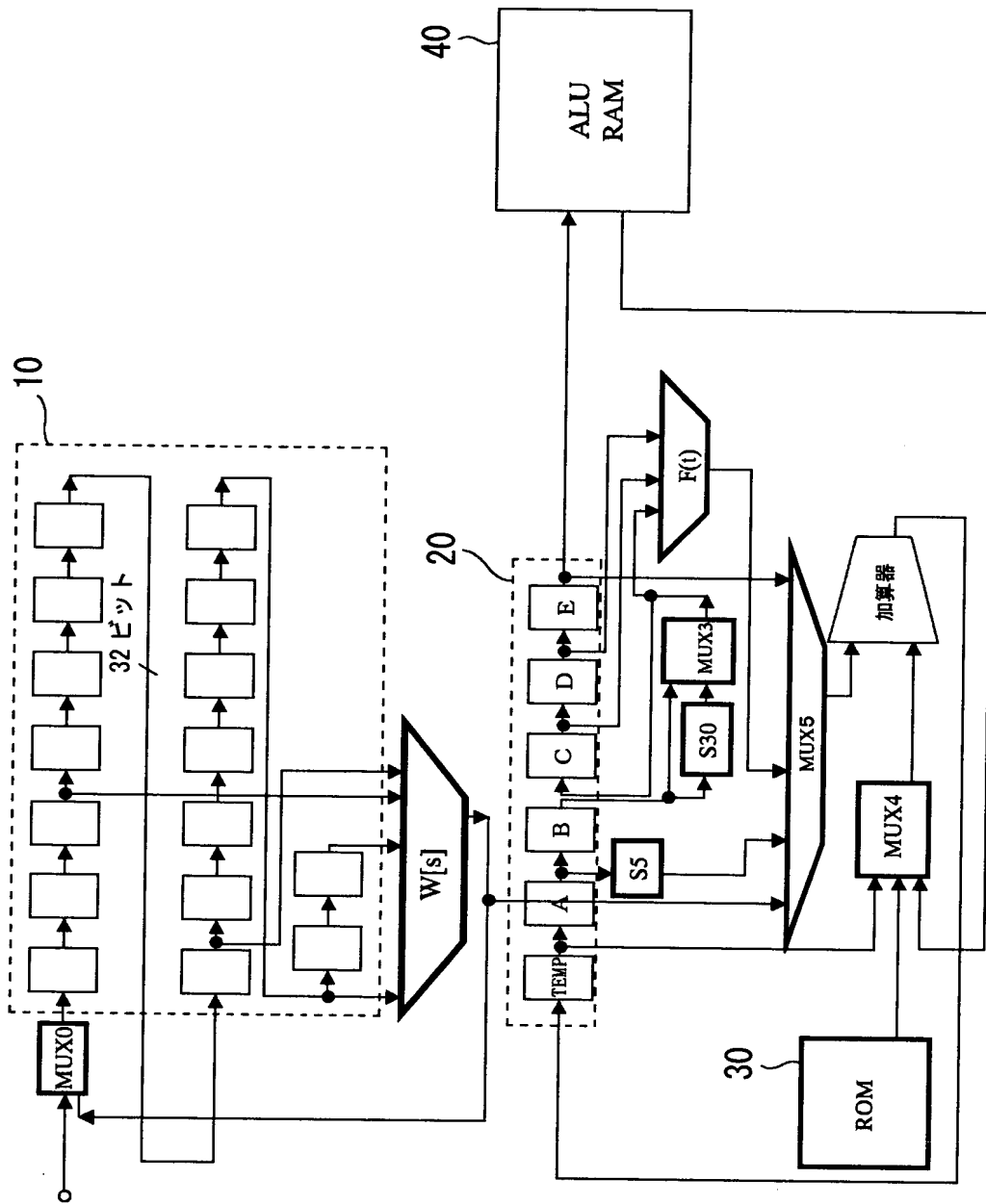
(A)



(C)

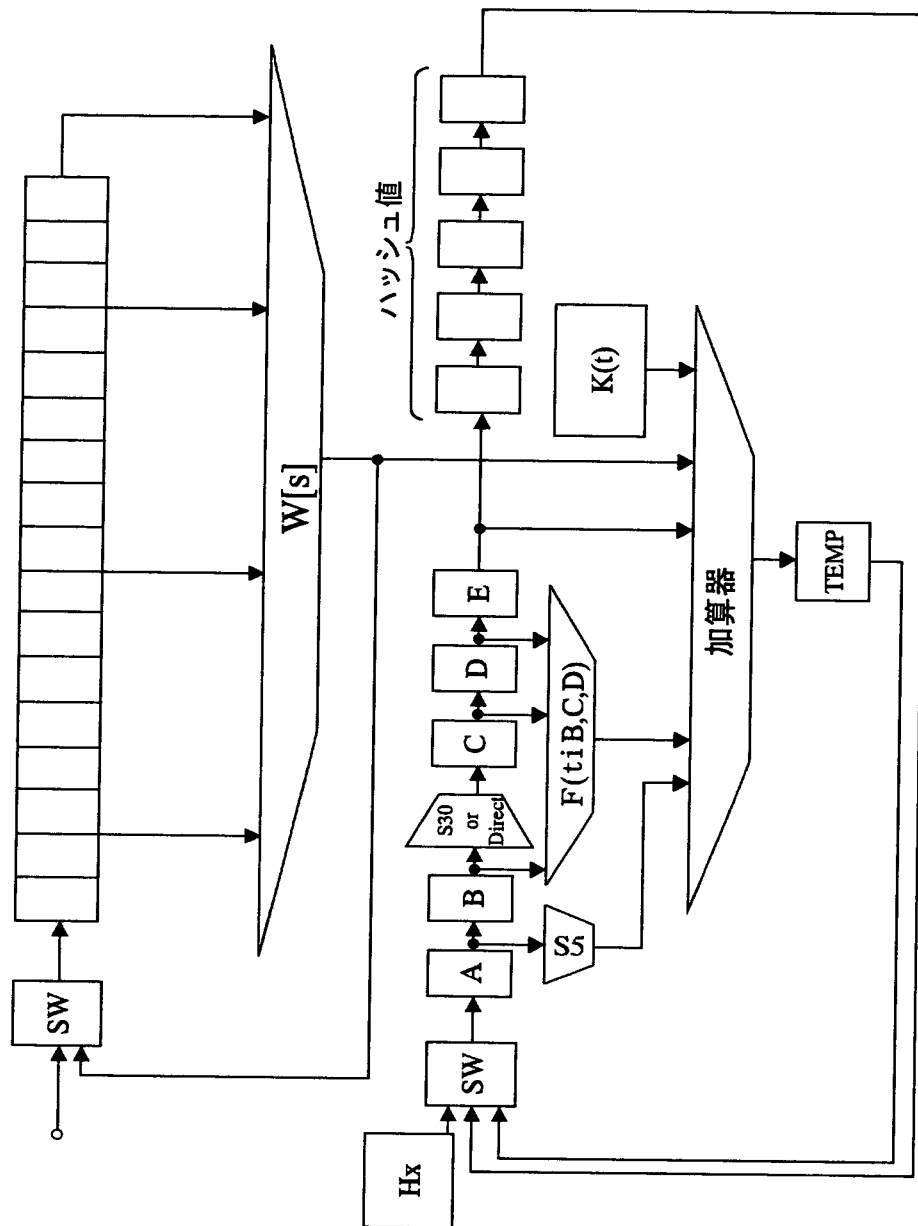
暗号化装置の概念図

【図2】



SHA-1 処理回路の構成ブロック図

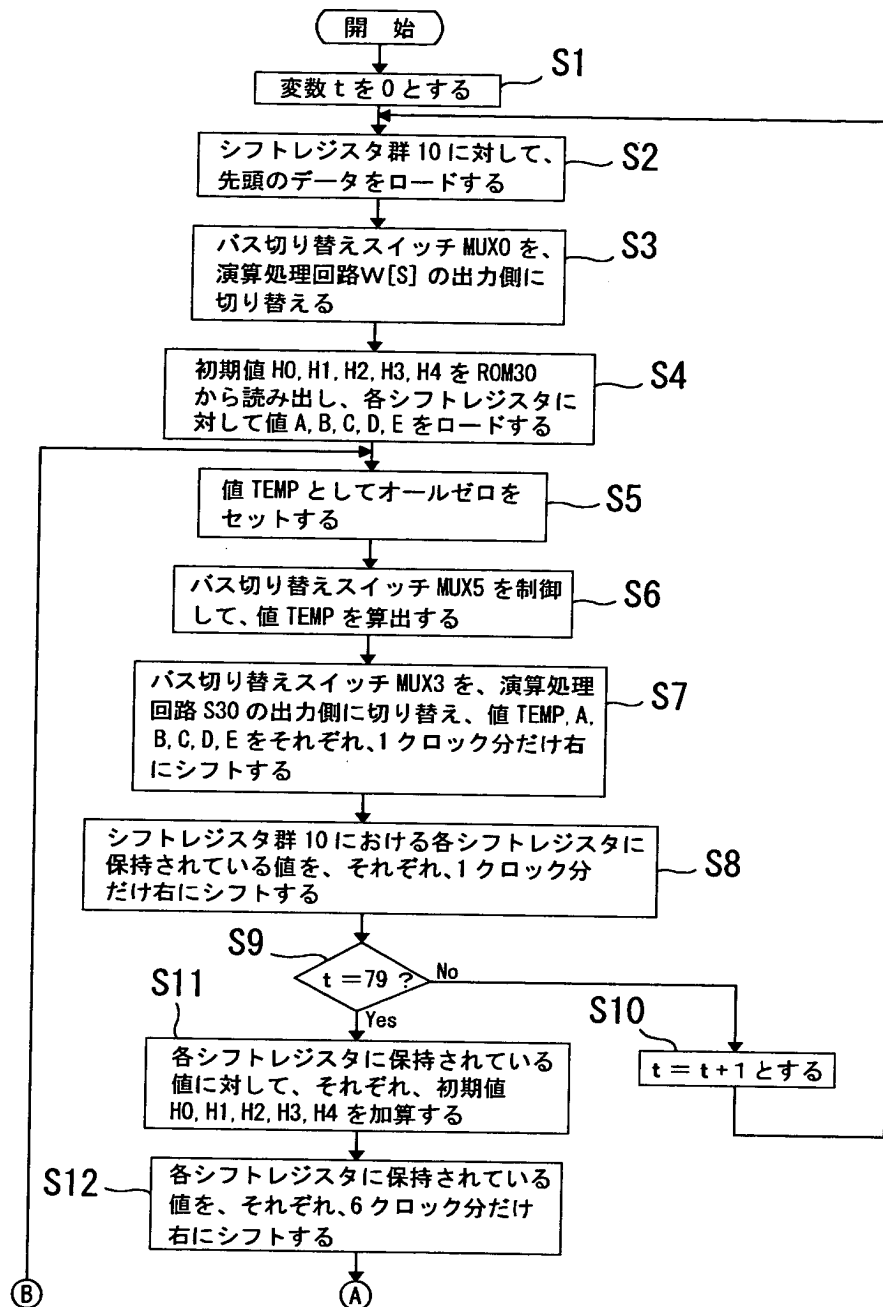
【図 3】



SHA-1 処理回路の構成ブロック図

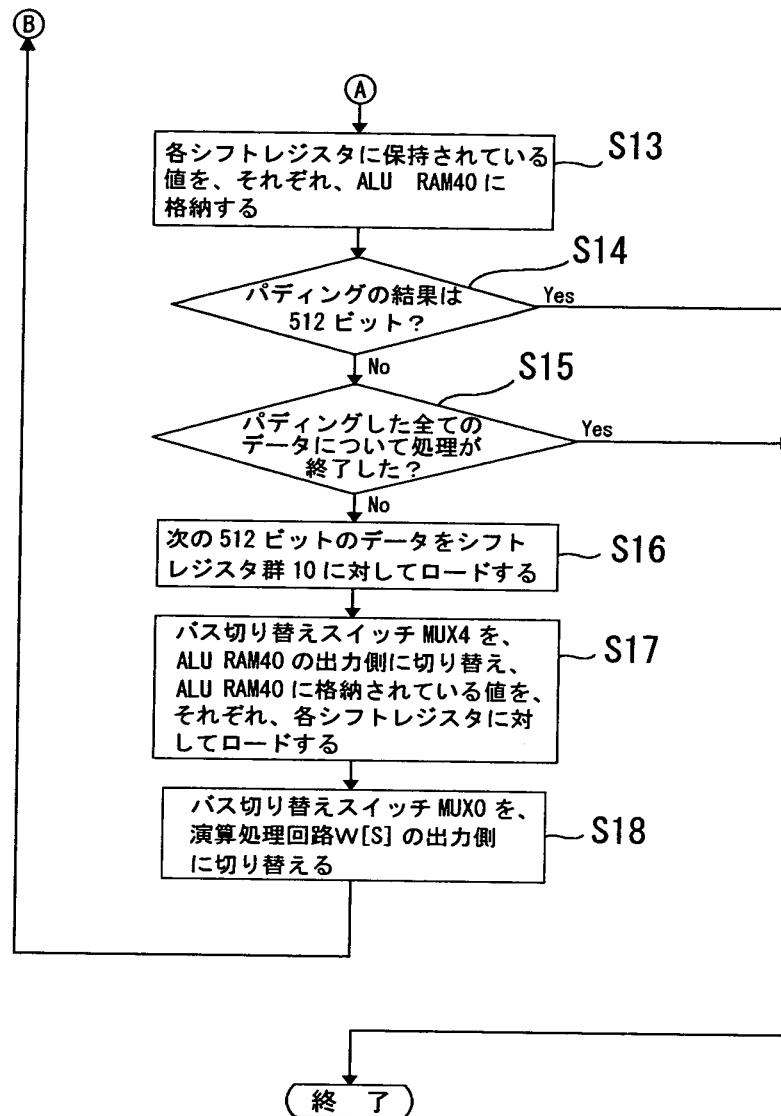


【図4】



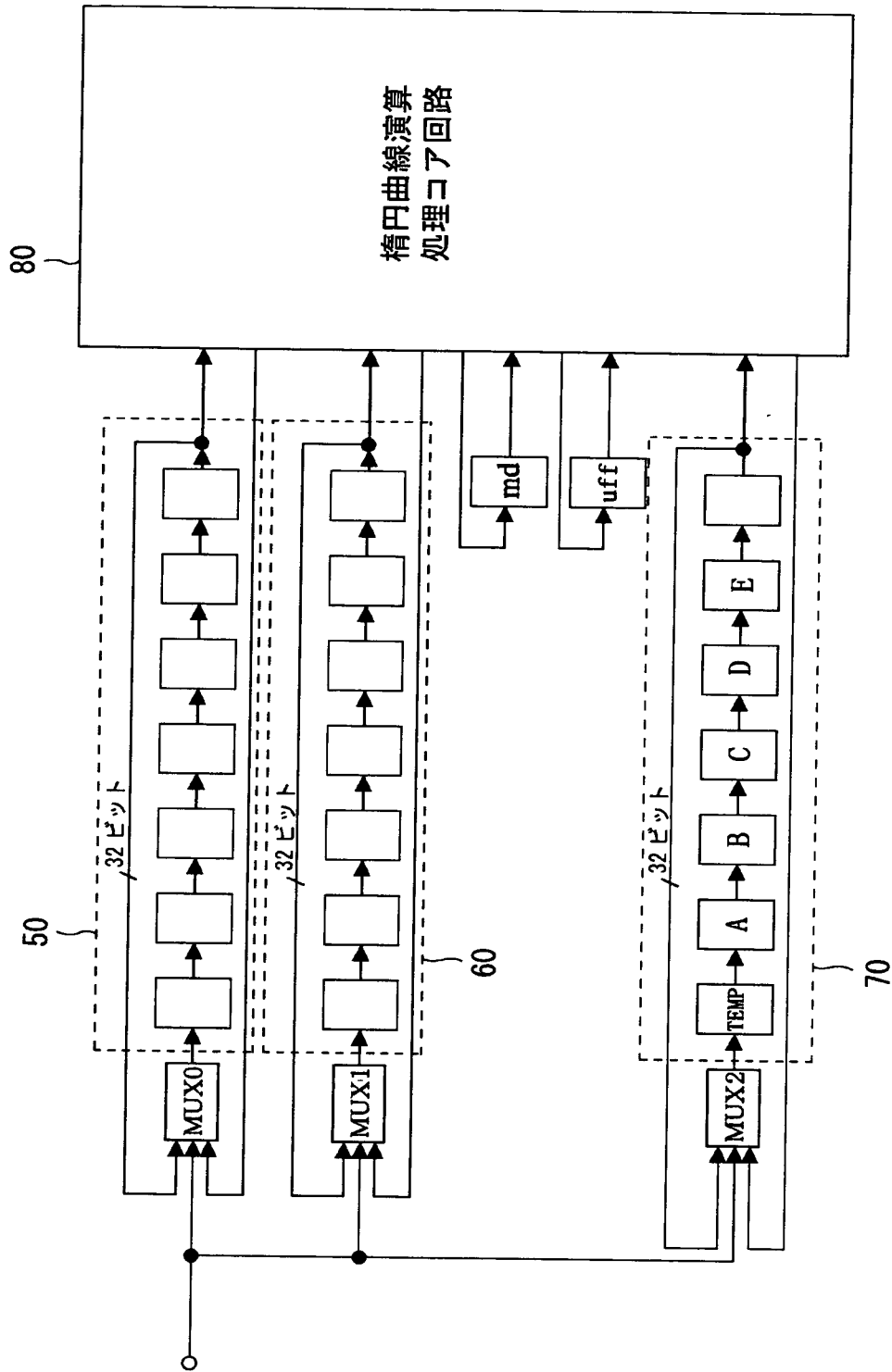
SHA-1 処理回路における一連の処理工程

【図 5】



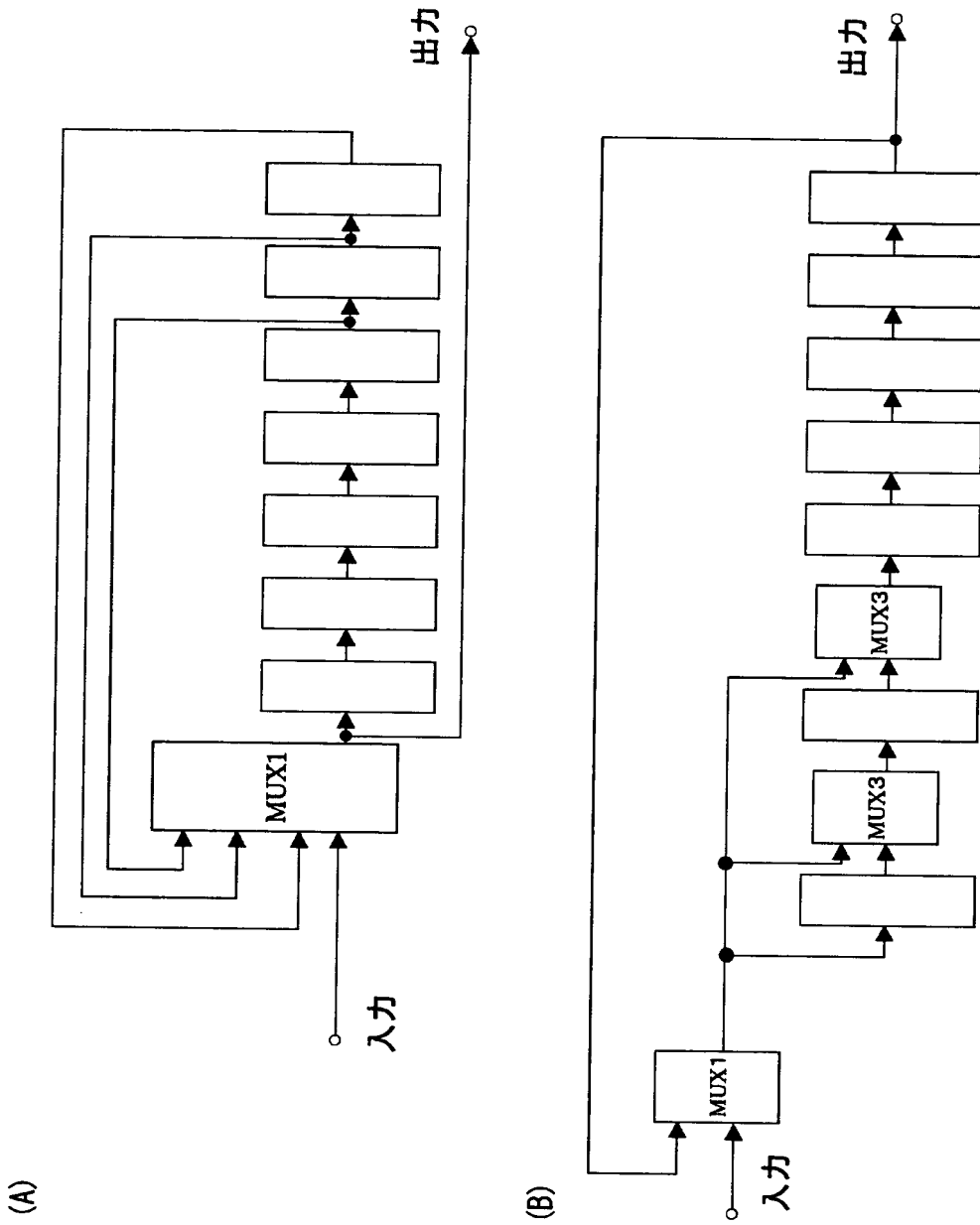
SHA-1 処理回路における一連の処理工程

【図6】



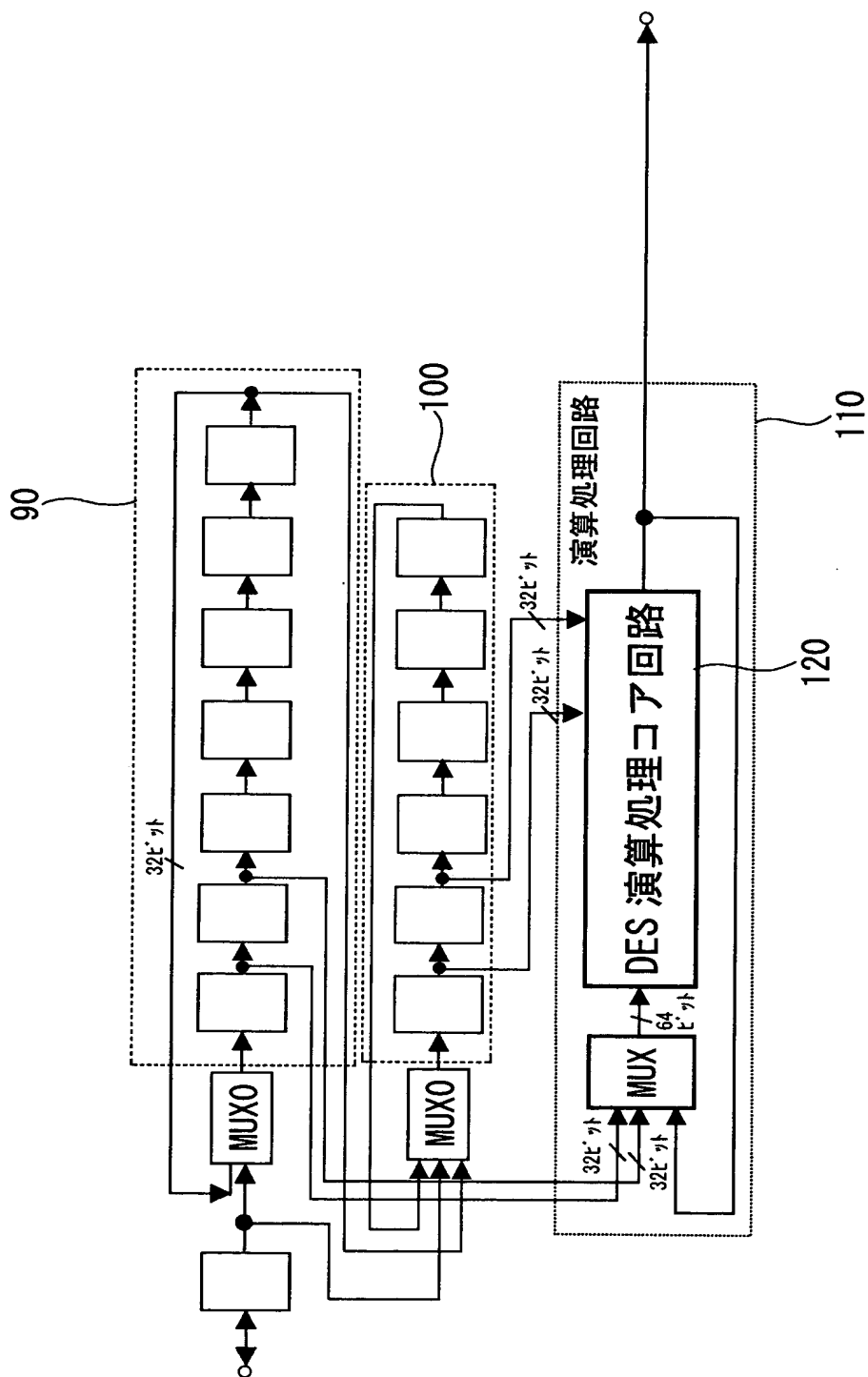
楕円曲線暗号化処理回路の構成ブロック図

【図 7】



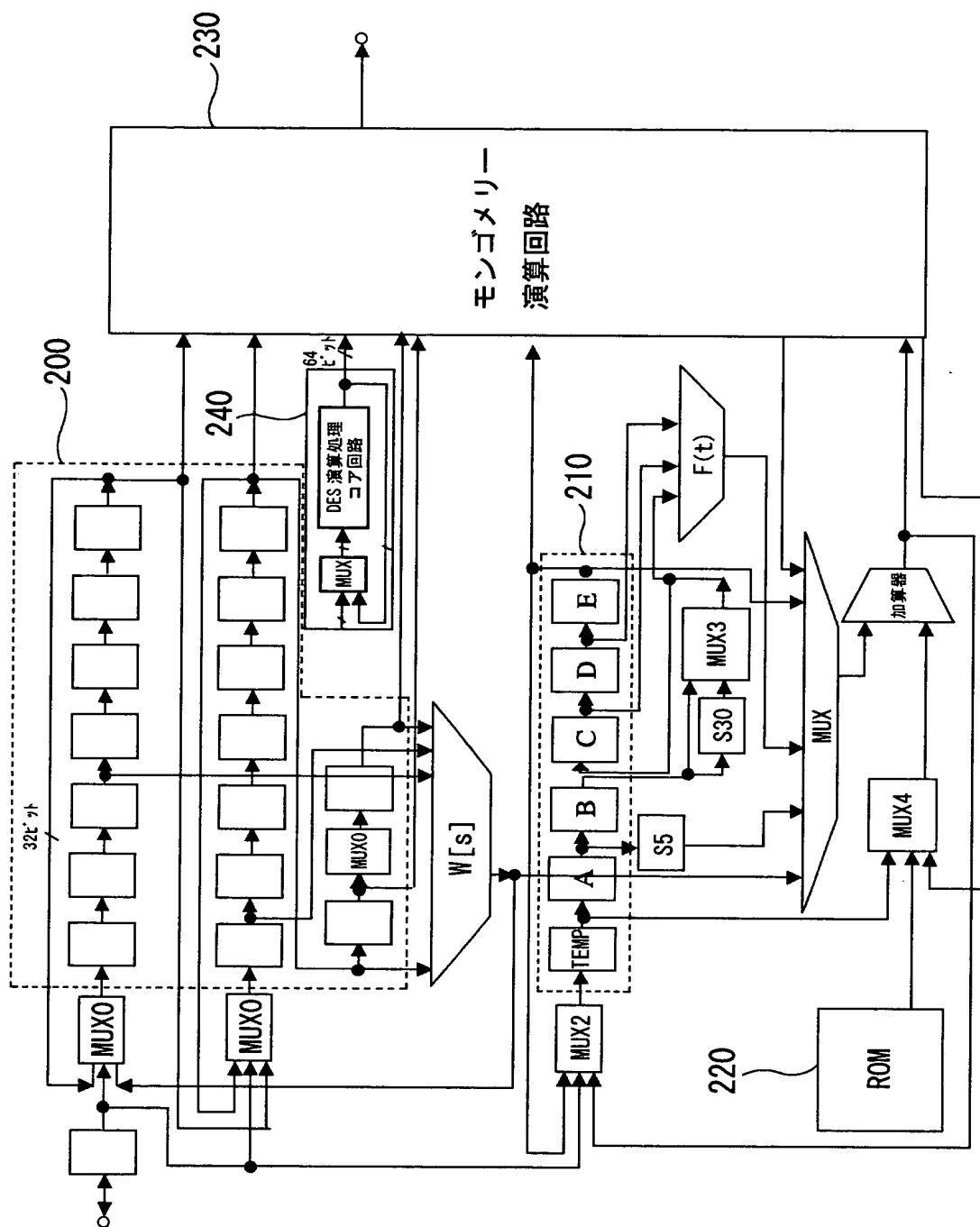
楕円曲線暗号化処理回路の要部構成ブロック図

【図 8】



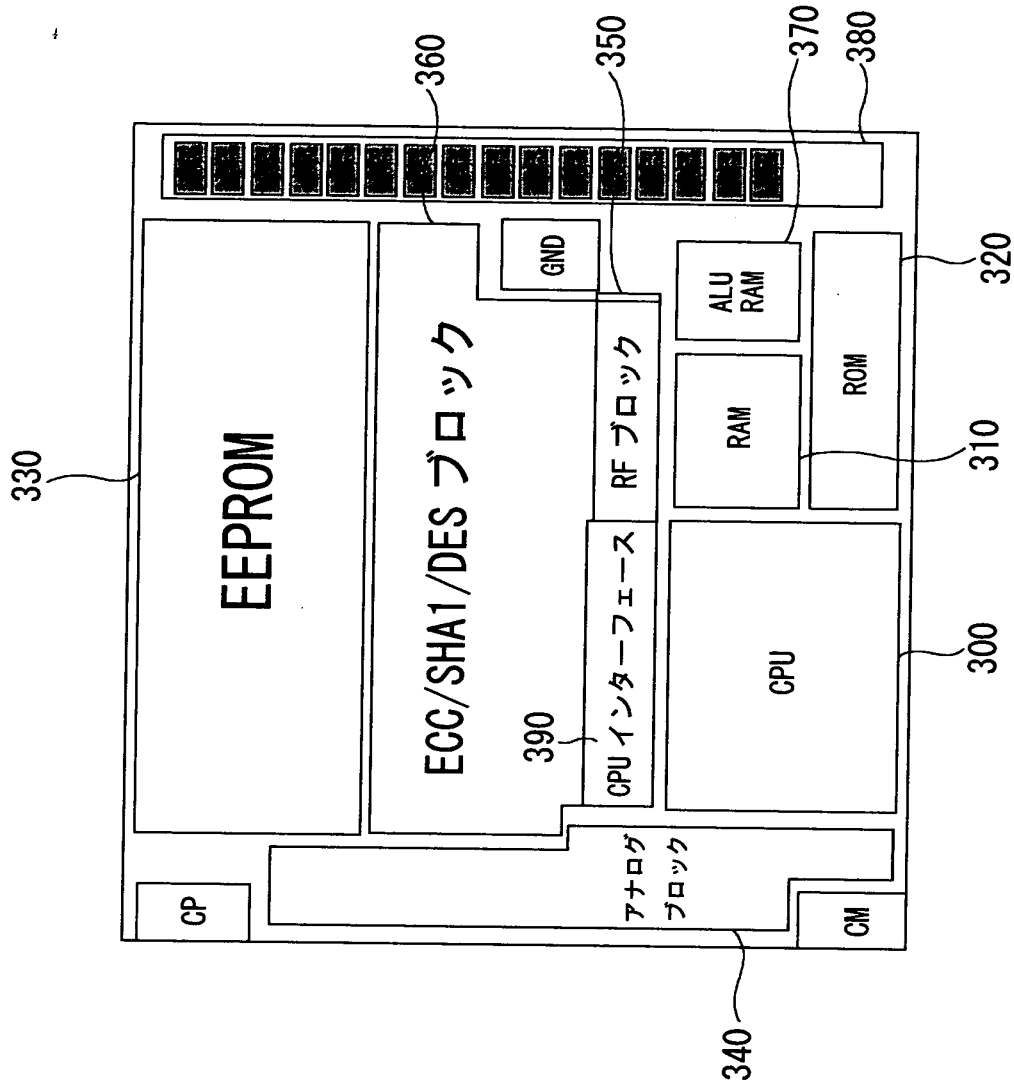
DES 暗号化処理回路の構成ブロック図

【図9】



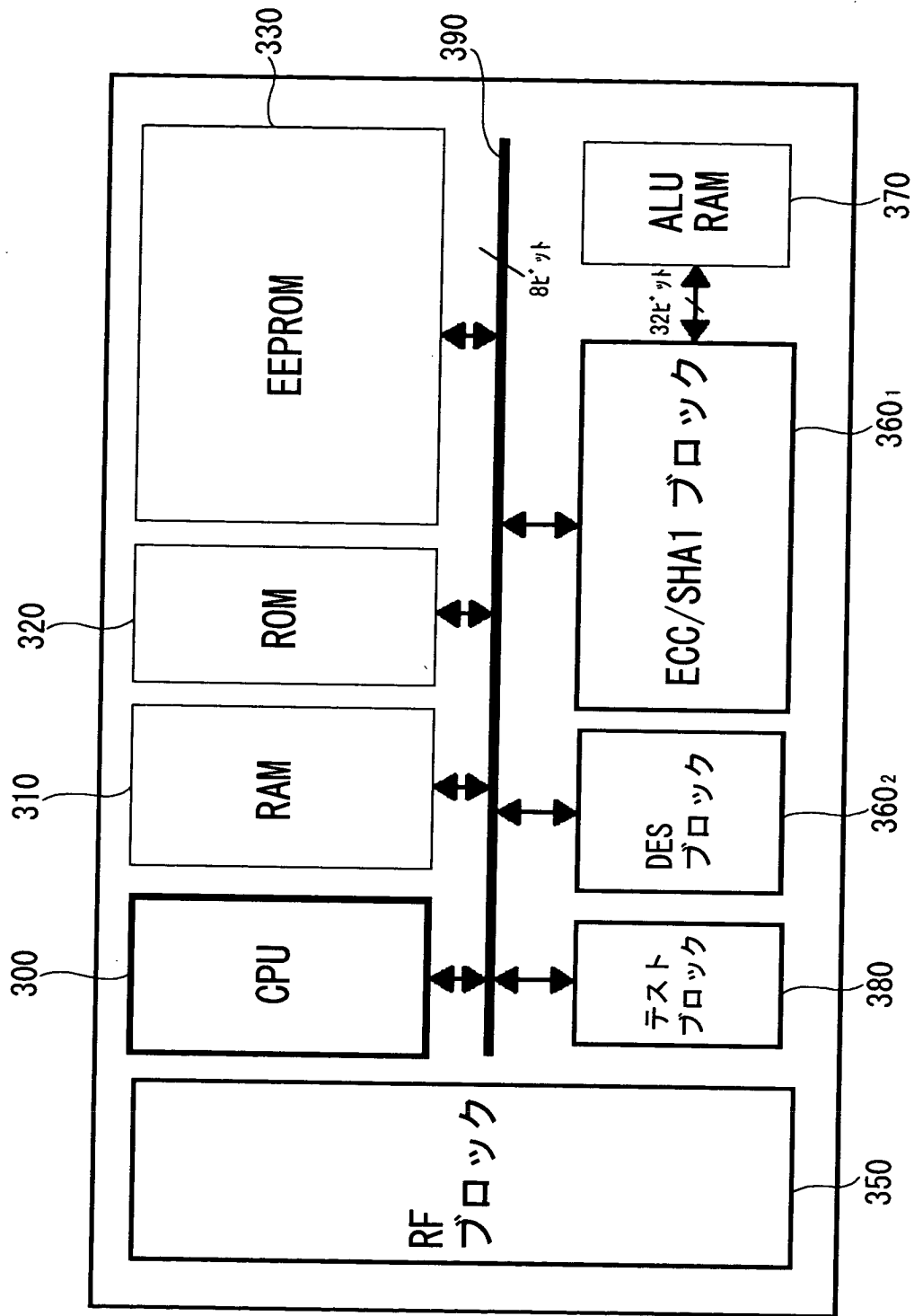
暗号化装置の構成ブロック図

【図10】



非接触型 IC カードの構成ブロック図

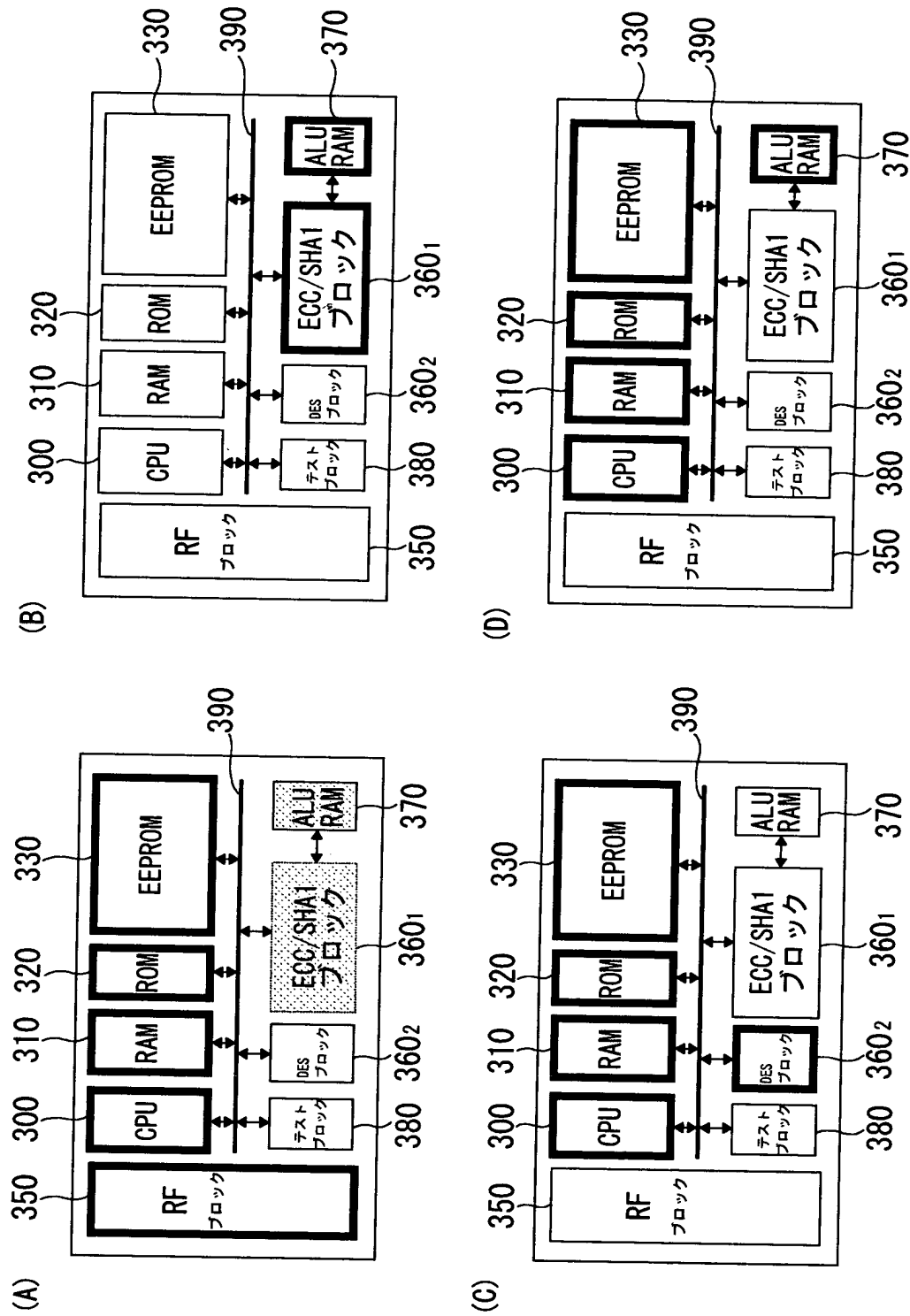
【図11】



非接触型 IC カードの構成ブロック図



【図 1 2】



非接触型 IC カードの動作の説明図

【書類名】 要約書

【要約】

【課題】 回路規模を削減し、極めて少ない電力消費のもとに高速且つ安全に公開鍵を用いた署名生成及び署名検証を可能とする暗号化装置を提供する。

【解決手段】 暗号化装置は、少なくとも、公開鍵暗号化方式による暗号化処理に用いるハッシュ値を生成する際の演算用の値を保持するためのシフトレジスタ及び結果としてのハッシュ値を取り込むためのシフトレジスタからなるシフトレジスタ群と、公開鍵暗号化方式による暗号化処理を行う際の演算用の値を保持するためのシフトレジスタ及び結果を取り込むためのシフトレジスタからなるシフトレジスタ群とを、シフトレジスタ群 2 0 0, 2 1 0 として共用し、処理モードに応じて、動作させるハードウェアを時分割に切り替える。

【選択図】 図 9

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日  
[変更理由] 新規登録  
住 所 東京都品川区北品川6丁目7番35号  
氏 名 ソニー株式会社